

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-139998

(P2002-139998A)

(43) 公開日 平成14年5月17日 (2002.5.17)

(51) Int. Cl.	識別記号	F I	テグト* (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 Z 5 B 0 4 9
			6 4 0 B 5 C 0 6 4
G 0 6 F 17/60	Z E C	G 0 6 F 17/60	Z E C 5 J 1 0 4
	1 4 0		1 4 0
	3 0 2		3 0 2 E

審査請求 未請求 請求項の数24 OL (全 87 頁) 最終頁に続く

(21) 出願番号 特願2000-334186 (P2000-334186)

(22) 出願日 平成12年11月1日 (2000.11.1)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 石橋 義人

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(72) 発明者 吉野 賢治

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

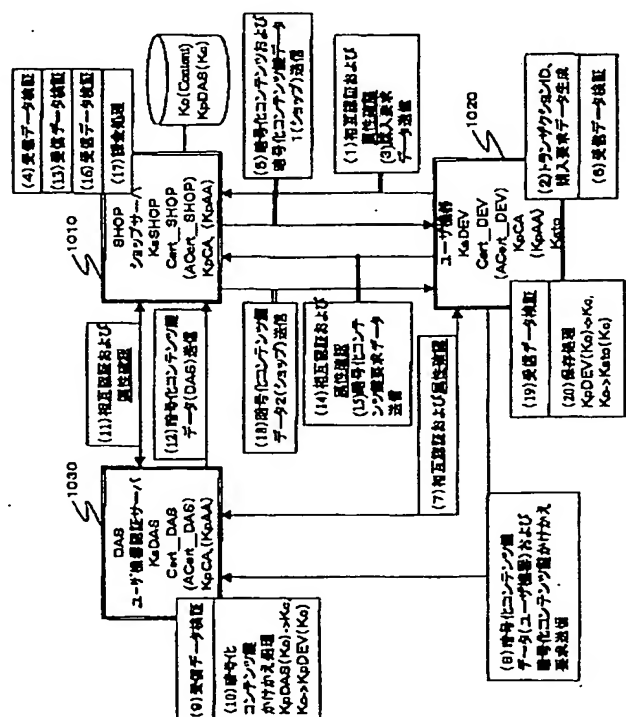
最終頁に続く

(54) 【発明の名称】 属性確認処理を含むデータ通信システムおよび属性確認処理を含むデータ通信方法

(57) 【要約】

【課題】 データ通信を安全に行なうことを可能とした属性確認処理を含むデータ通信システムを提供する。

【解決手段】 データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を通信相手のエンティティの公開鍵証明書または属性証明書から取得し、取得した属性情報に基づく属性確認がなされたことを処理実行条件とする。例えば、コンテンツの購入を実行するユーザ機器、コンテンツの購入要求を受け付けるショップサーバ、コンテンツ配信管理を行うシステムホルダ等の機能毎に異なる属性コードを付与して、属性コードに基づいて属性確認を実行する。本構成によれば、通信相手が他のエンティティになりすまして処理を実行することが防止され、安全なコンテンツ取り引き等のデータ通信が可能となる。



【特許請求の範囲】

【請求項1】データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を該通信相手のエンティティの公開鍵証明書または属性証明書から取得し、取得した属性情報に基づく属性確認がなされたことを処理実行条件とした構成を有することを特徴とする属性確認処理を含むデータ通信システム。

【請求項2】前記属性情報は、エンティティの機能に基づいて設定される属性情報であることを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項3】データ通信を実行するエンティティは、コンテンツ配信システムを構成するエンティティであつて、

コンテンツを購入する機能を持つユーザ機器、コンテンツの購入依頼を受領する機能を持つショップサーバ、コンテンツ配信を管理する機能を持つサービス運営体サーバ、コンテンツを配信する配信サーバ中の2以上のエンティティを含み、該異なるエンティティの各々には、異なる属性情報としての属性コードが付与され、各エンティティの公開鍵証明書または属性証明書に格納された構成であることを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項4】前記エンティティの属性情報は、当該エンティティの公開鍵証明書に格納され、属性情報を格納した公開鍵証明書には、公開鍵証明書発行局の署名が生成されて格納された構成を有することを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項5】前記エンティティの属性情報は、当該エンティティの属性証明書に格納され、属性情報を格納した属性証明書には、属性証明書発行局の署名が生成されて格納された構成を有することを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項6】データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、エンティティ間の相互認証処理において取得する通信相手の公開鍵証明書から取得する処理として実行することを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項7】データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、通信相手の属性証明書を取得し、属性証明書中の属性証明書発行局の署名検証を実行し、署名検証成功を条件として属性証明書から取得する処理として実行することを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項8】データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、

受信データの署名検証処理に適用する通信相手エンティティの公開鍵証明書から取得する処理として実行することを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項9】データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、

通信相手の公開鍵証明書とリンクする属性証明書を、公開鍵証明書および属性証明書に共通に格納された公開鍵証明書通し番号に基づいて確認し、公開鍵証明書と同一の公開鍵証明書通し番号を格納した属性証明書から取得する処理として実行することを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項10】前記属性確認処理は、通信相手のエンティティの公開鍵証明書、または属性証明書から取得した属性コードと、通信相手として想定したエンティティに設定された属性コードとの比較処理として実行する構成であることを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項11】前記属性確認処理は、特定の通信相手に固有の通信処理実行シーケンスに含まれる属性コード比較処理であり、前記特定の通信相手に設定された属性コードと、通信相手のエンティティの公開鍵証明書、または属性証明書から取得した属性コードとの比較処理として実行する構成であることを特徴とする請求項1に記載の属性確認処理を含むデータ通信システム。

【請求項12】データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を該通信相手のエンティティの公開鍵証明書または属性証明書から取得する属性情報取得ステップと、前記属性情報取得ステップにおいて取得した属性情報に基づく属性確認を実行する属性確認処理ステップとを有し、前記属性確認ステップにおいて属性の正当性が確認されたことを次処理実行条件としたことを特徴とする属性確認処理を含むデータ通信方法。

【請求項13】前記属性情報は、エンティティの機能に基づいて設定される属性情報であることを特徴とする請求項12に記載の属性確認処理を含むデータ通信方法。

【請求項14】データ通信を実行するエンティティは、コンテンツ配信システムを構成するエンティティであつて、

コンテンツを購入する機能を持つユーザ機器、コンテンツの購入依頼を受領する機能を持つショップサーバ、コンテンツ配信を管理する機能を持つサービス運営体サーバ、コンテンツを配信する配信サーバ中の2以上のエンティティを含み、該異なるエンティティの各々には、異なる属性情報としての属性コードが付与され、各エンティティの公開鍵証明書または属性証明書に格納され、

前記公開鍵証明書または属性証明書に基づく属性確認を実行することを特徴とする請求項12に記載の属性確認処理を含むデータ通信方法。

【請求項15】前記エンティティの公開鍵証明書は、エンティティに設定された属性情報を含み、公開鍵証明書発行局の署名が格納され、

属性確認を実行するエンティティは、前記公開鍵証明書発行局の署名検証の後、前記属性情報を取得する処理を実行することを特徴とする請求項12に記載の属性確認処理を含むデータ通信方法。

【請求項16】前記エンティティの属性証明書は、エンティティに設定された属性情報を含み、属性証明書発行局の署名が格納され、

属性確認を実行するエンティティは、前記属性証明書発行局の署名検証の後、前記属性情報を取得する処理を実行することを特徴とする請求項12に記載の属性確認処理を含むデータ通信方法。

【請求項17】データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、

エンティティ間の相互認証処理において取得する通信相手の公開鍵証明書から取得する処理として実行することを特徴とする請求項12に記載の属性確認処理を含むデータ通信方法。

【請求項18】データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、

受信データの署名検証処理に適用する通信相手エンティティの公開鍵証明書から取得する処理として実行することを特徴とする請求項12に記載の属性確認処理を含むデータ通信方法。

【請求項19】データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、

通信相手の公開鍵証明書とリンクする属性証明書を、公開鍵証明書および属性証明書に共通に格納された公開鍵証明書通し番号に基づいて確認し、公開鍵証明書と同一の公開鍵証明書通し番号を格納した属性証明書から取得する処理として実行することを特徴とする請求項12に記載の属性確認処理を含むデータ通信方法。

【請求項20】前記属性確認処理ステップは、通信相手のエンティティの公開鍵証明書、または属性証明書から取得した属性コードと、通信相手として想定したエンティティに設定された属性コードとの比較処理として実行することを特徴とする請求項12に記載の属性確認処理を含むデータ通信方法。

【請求項21】前記属性確認処理ステップは、特定の通信相手に固有の通信処理実行プログラムに含まれる属性コード比較処理であり、前記特定の通信相手に設定された属性コードと、通信相

手のエンティティの公開鍵証明書、または属性証明書から取得した属性コードとの比較処理として実行することを特徴とする請求項12に記載の属性確認処理を含むデータ通信方法。

【請求項22】データ通信を実行するエンティティの機能に基づく属性情報を構成データとして有するとともに、公開鍵証明所発行局の署名データを含む公開鍵証明書を格納したことを特徴とする記録媒体。

【請求項23】データ通信を実行するエンティティの機能に基づく属性情報を構成データとして有するとともに、属性証明書発行局の署名データを含む属性証明書を格納したことを特徴とする記録媒体。

【請求項24】データ通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を通信相手のエンティティの公開鍵証明書または属性証明書から取得する属性情報取得ステップと、

前記属性情報取得ステップにおいて取得した属性情報に基づく属性確認を実行する属性確認処理ステップと、を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は属性確認処理を含むデータ通信システムおよび属性確認処理を含むデータ通信方法に関する。さらに、詳細には、データ通信を実行するエンティティ間において通信相手の属性確認を実行することにより、セキュリティの高い正当なコンテンツ流通処理等のデータ通信処理を実行することを可能とした属性確認処理を含むデータ通信システムおよび属性確認処理を含むデータ通信方法に関する。

【0002】

【従来の技術】昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）の、インターネット等、ネットワークを介した流通が盛んになってきている。また、オンラインショッピング、銀行決済、チケット販売等のネットワークを介した商品売買、決済処理等も盛んになってきている。

【0003】このようなネットワークを介したデータ通信においては、データ送信側とデータ受信側とが互いに正規なデータ送受信対象であることを確認した上で、必要な情報を転送する、すなわちセキュリティを考慮したデータ転送構成をとるのが一般的となっている。データ転送の際のセキュリティ構成を実現する手法には、転送データの暗号化処理、データに対する署名処理等がある。

【0004】暗号化データは、所定の手続きによる復号

化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【0005】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる公開鍵暗号方式と呼ばれる方式がある。公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。例えば、データ暗号化鍵を公開鍵とし、復号鍵を秘密鍵とする。あるいは、認証子生成鍵を秘密鍵とし、認証子検証鍵を公開鍵とする等の態様において使用される。

【0006】暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号化方式と異なり、公開鍵暗号方式では秘密に保つ必要のある秘密鍵は、特定の1人が持てばよいため鍵の管理において有利である。ただし、公開鍵暗号方式は共通鍵暗号化方式に比較してデータ処理速度が遅く、秘密鍵の配送、デジタル署名等のデータ量の少ない対象に多く用いられている。公開鍵暗号方式の代表的なものにはRSA（Rivest-Shamir-Adleman）暗号がある。これは非常に大きな2つの素数（例えば150桁）の積を用いるものであり、大きな2つの素数（例えば150桁）の積の素因数分解する処理の困難さを利用して

【0007】公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者Aが公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者Aは公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者Aに送付する。利用者Aは秘密鍵を用いて暗号化文書等を復号する等のシステムである。また、利用者Aは、秘密鍵を用いて文書等に署名を付け、不特定のユーザが公開鍵証明書から所定の手続きを経て公開鍵を入手して、その署名の検証を行なうシステムである。

【0008】公開鍵証明書は、公開鍵暗号方式における認証局あるいは発行局（CA：Certificate Authority またはIA：Issuer Authority）が発行する証明書であり、ユーザが自己のID、公開鍵等を認証局に提出することにより、認証局側が認証局のIDや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【0009】公開鍵証明書は、証明書のバージョン番号、発行局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の

名前（ユーザID）、証明書利用者の公開鍵並びに電子署名を含む。

【0010】電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

【0011】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【0012】

【発明が解決しようとする課題】上述のような認証局発行の公開鍵証明書を用いた公開鍵暗号方式によるデータ送信システムにおいては、例えばコンテンツを配信するコンテンツ配信ショップは、ユーザの公開鍵に基づいて配信対象のコンテンツを暗号化してユーザに送信する。コンテンツ配信ショップからの暗号化データを受信したユーザ機器は、自己の公開鍵に対応する自己の秘密鍵で暗号化コンテンツの復号を実行する。

【0013】しかし、コンテンツ取り引きにおいてデータ通信を実行する場合、通信相手がショップであるのか、ユーザ機器であるのか、あるいはその他システムホルダ等の管理サーバであるのかを確認することは困難である。通信相手から送信されるデータに基づいて判定するしかないのが現状である。

【0014】従って、不正なユーザ機器、不正なショップ等が存在し、不正なユーザ機器がショップになりすましてコンテンツの架空取引を実行したりする可能性がある。また、正当な取引を実行しようとするユーザ機器がショップサーバであると信じて通信を開始し、ショップサーバ相手のコンテンツ購入要求を実行して、例えばクレジット口座番号の送信処理を実行するような場合、相手がショップサーバになりすました不正なサーバであるような場合は、ユーザ機器からクレジット口座番号を不正に取得する等の処理が実行されるおそれがある。

【0015】また、不正、あるいは架空のコンテンツ取り引きが実行されると、コンテンツの取り引き実体の把握が困難となる。一般的には、コンテンツ配信ショップの自己申告により、コンテンツの販売量を確認し、自己申告に基づくライセンス料が、ショップからライセンスホルダ、あるいはコンテンツ製作者等に提供されるのが一般的な取り引き形態であるが、不正、あるいは架空のコンテンツ取り引きが実行されると、ショップにおいて

も、また、コンテンツの頒布権を持つライセンスホルダ、あるいはコンテンツの著作権を持つコンテンツ製作者も正当なコンテンツ取引に伴うライセンス料の取得が保証されない。

【0016】本発明は、上述のような、コンテンツ取引における問題点に鑑みてなされたものであり、データ通信を実行するエンティティ間において、通信相手のエンティティの属性を確認して処理を実行することにより、不正な相手との処理、例えばコンテンツ購入に伴う様々な処理が不正に実行されることを防止可能とした属性確認処理を含むデータ通信システムおよび属性確認処理を含むデータ通信方法を実現することを目的とする。

【0017】より具体的には、例えばコンテンツを購入する機能を持つユーザ機器、コンテンツの購入依頼を受領する機能を持つショップサーバ、コンテンツ配信を管理する機能を持つサービス運営体サーバ、コンテンツを配信する配信サーバ等の異なるエンティティの各々に、異なる属性情報としての属性コードを付与し、各エンティティの公開鍵証明書または属性証明書に格納された属性情報によって通信相手の確認を可能として暗然なコンテンツ取引形態を実現する属性確認処理を含むデータ通信システムおよび属性確認処理を含むデータ通信方法を提供することを目的とする。

【0018】

【課題を解決するための手段】本発明の第1の側面は、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を該通信相手のエンティティの公開鍵証明書または属性証明書から取得し、取得した属性情報に基づく属性確認がなされたことを処理実行条件とした構成を有することを特徴とする属性確認処理を含むデータ通信システムにある。

【0019】さらに、本発明のデータ通信システムの一実施態様において、前記属性情報は、エンティティの機能に基づいて設定される属性情報であることを特徴とする。

【0020】さらに、本発明のデータ通信システムの一実施態様において、データ通信を実行するエンティティは、コンテンツ配信システムを構成するエンティティであって、コンテンツを購入する機能を持つユーザ機器、コンテンツの購入依頼を受領する機能を持つショップサーバ、コンテンツ配信を管理する機能を持つサービス運営体サーバ、コンテンツを配信する配信サーバ中の2以上のエンティティを含み、該異なるエンティティの各々には、異なる属性情報としての属性コードが付与され、各エンティティの公開鍵証明書または属性証明書に格納された構成であることを特徴とする。

【0021】さらに、本発明のデータ通信システムの一実施態様において、前記エンティティの属性情報は、当該エンティティの公開鍵証明書に格納され、属性情報を格納した公開鍵証明書には、公開鍵証明書発行局の署名

が生成されて格納された構成を有することを特徴とする。

【0022】さらに、本発明のデータ通信システムの一実施態様において、前記エンティティの属性情報は、当該エンティティの属性証明書に格納され、属性情報を格納した属性証明書には、属性証明書発行局の署名が生成されて格納された構成を有することを特徴とする。

【0023】さらに、本発明のデータ通信システムの一実施態様において、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、エンティティ間の相互認証処理において取得する通信相手の公開鍵証明書から取得する処理として実行することを特徴とする。

【0024】さらに、本発明のデータ通信システムの一実施態様において、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、通信相手の属性証明書を取得し、属性証明書中の属性証明書発行局の署名検証を実行し、署名検証成功を条件として属性証明書から取得する処理として実行することを特徴とする。

【0025】さらに、本発明のデータ通信システムの一実施態様において、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、受信データの署名検証処理に適用する通信相手エンティティの公開鍵証明書から取得する処理として実行することを特徴とする。

【0026】さらに、本発明のデータ通信システムの一実施態様において、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、通信相手の公開鍵証明書とリンクする属性証明書を、公開鍵証明書および属性証明書に共通に格納された公開鍵証明書通し番号に基づいて確認し、公開鍵証明書と同一の公開鍵証明書通し番号を格納した属性証明書から取得する処理として実行することを特徴とする。

【0027】さらに、本発明のデータ通信システムの一実施態様において、前記属性確認処理は、通信相手のエンティティの公開鍵証明書、または属性証明書から取得した属性コードと、通信相手として想定したエンティティに設定された属性コードとの比較処理として実行する構成であることを特徴とする。

【0028】さらに、本発明のデータ通信システムの一実施態様において、前記属性確認処理は、特定の通信相手に固有の通信処理実行シーケンスに含まれる属性コード比較処理であり、前記特定の通信相手に設定された属性コードと、通信相手のエンティティの公開鍵証明書、または属性証明書から取得した属性コードとの比較処理として実行する構成であることを特徴とする。

【0029】さらに、本発明の第2の側面は、データ通信を実行するエンティティ間において、通信相手のエン

ティティに設定された属性情報を該通信相手のエンティティの公開鍵証明書または属性証明書から取得する属性情報取得ステップと、前記属性情報取得ステップにおいて取得した属性情報に基づく属性確認を実行する属性確認処理ステップとを有し、前記属性確認ステップにおいて属性の正当性が確認されたことを次処理実行条件としたことを特徴とする属性確認処理を含むデータ通信方法にある。

【0030】さらに、本発明のデータ通信方法の一実施態様において、前記属性情報は、エンティティの機能に基づいて設定される属性情報であることを特徴とする。

【0031】さらに、本発明のデータ通信方法の一実施態様において、データ通信を実行するエンティティは、コンテンツ配信システムを構成するエンティティであって、コンテンツを購入する機能を持つユーザ機器、コンテンツの購入依頼を受領する機能を持つショップサーバ、コンテンツ配信を管理する機能を持つサービス運営体サーバ、コンテンツを配信する配信サーバ中の2以上のエンティティを含み、該異なるエンティティの各々には、異なる属性情報としての属性コードが付与され、各エンティティの公開鍵証明書または属性証明書に格納され、前記公開鍵証明書または属性証明書に基づく属性確認を実行することを特徴とする。

【0032】さらに、本発明のデータ通信方法の一実施態様において、前記エンティティの公開鍵証明書は、エンティティに設定された属性情報を含み、公開鍵証明書発行局の署名が格納され、属性確認を実行するエンティティは、前記公開鍵証明書発行局の署名検証の後、前記属性情報を取得する処理を実行することを特徴とする。

【0033】さらに、本発明のデータ通信方法の一実施態様において、前記エンティティの属性証明書は、エンティティに設定された属性情報を含み、属性証明書発行局の署名が格納され、属性確認を実行するエンティティは、前記属性証明書発行局の署名検証の後、前記属性情報を取得する処理を実行することを特徴とする。

【0034】さらに、本発明のデータ通信方法の一実施態様において、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、エンティティ間の相互認証処理において取得する通信相手の公開鍵証明書から取得する処理として実行することを特徴とする。

【0035】さらに、本発明のデータ通信方法の一実施態様において、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を取得する処理は、受信データの署名検証処理に適用する通信相手エンティティの公開鍵証明書から取得する処理として実行することを特徴とする。

【0036】さらに、本発明のデータ通信方法の一実施態様において、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報

を取得する処理は、通信相手の公開鍵証明書とリンクする属性証明書を、公開鍵証明書および属性証明書に共通に格納された公開鍵証明書通し番号に基づいて確認し、公開鍵証明書と同一の公開鍵証明書通し番号を格納した属性証明書から取得する処理として実行することを特徴とする。

【0037】さらに、本発明のデータ通信方法の一実施態様において、前記属性確認処理ステップは、通信相手のエンティティの公開鍵証明書、または属性証明書から取得した属性コードと、通信相手として想定したエンティティに設定された属性コードとの比較処理として実行することを特徴とする。

【0038】さらに、本発明のデータ通信方法の一実施態様において、前記属性確認処理ステップは、特定の通信相手に固有の通信処理実行プログラムに含まれる属性コード比較処理であり、前記特定の通信相手に設定された属性コードと、通信相手のエンティティの公開鍵証明書、または属性証明書から取得した属性コードとの比較処理として実行することを特徴とする。

【0039】さらに、本発明の第3の側面は、データ通信を実行するエンティティの機能に基づく属性情報を構成データとして有するとともに、公開鍵証明所発行局の署名データを含む公開鍵証明書を格納したことを特徴とする記録媒体にある。

【0040】さらに、本発明の第4の側面は、データ通信を実行するエンティティの機能に基づく属性情報を構成データとして有するとともに、属性証明書発行局の署名データを含む属性証明書を格納したことを特徴とする記録媒体にある。

【0041】さらに、本発明の第5の側面は、データ通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を通信相手のエンティティの公開鍵証明書または属性証明書から取得する属性情報取得ステップと、前記属性情報取得ステップにおいて取得した属性情報に基づく属性確認を実行する属性確認処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【0042】なお、本発明の第5の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0043】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと

提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0044】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0045】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。なお、説明は、以下の項目に従って行なう。

1. 暗号化コンテンツ鍵の鍵かけかえ処理によるコンテンツ配信管理

1. 1. システム構成：基本コンテンツ配信モデル1
1. 2. 基本コンテンツ配信モデル1の変形例
1. 3. 基本コンテンツ配信モデル2
2. 電子チケットを利用したコンテンツ配信モデル
3. ログ収集サーバによるコンテンツ配信管理
4. 属性データを記録した公開鍵証明書または属性証明書利用構成

【0046】

【実施例】[1. 暗号化コンテンツ鍵の鍵かけかえ処理によるコンテンツ配信管理]

[1. 1. システム構成：基本コンテンツ配信モデル1] 図1に本発明のコンテンツ配信システムおよびコンテンツ配信方法の一実施例の概要を説明する図を示す。なお、システムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0047】図1のコンテンツ配信システムは、ユーザ機器に対するコンテンツの配信サービスを行なうショップサーバ(SHOP)100、ショップサーバ100からのコンテンツ配信を受信するユーザ機器(DEVICE)200、さらに、正当なコンテンツ取り引き管理を行なう管理サーバとして機能するユーザ機器認証サーバ(DAS: Device Authentication Server)300を主構成要素とする。なお、図1の構成では、ショップサーバ100、ユーザ機器200、ユーザ機器認証サーバ300を1つずつ示しているが、実際のコンテンツ取り引き構成においては、図1に示す各構成要素が複数存在し、各コンテンツ取り引き毎に、様々なルートで情報が送受信される。図1は、1つのコンテンツ取り引きにおけるデータの流れを示しているものである。

【0048】(ショップサーバ) 図1のコンテンツ配信システムのショップサーバ100の構成を図2に示す。ショップサーバ100は、取り引き対象となるコンテンツをコンテンツキーで暗号化した暗号化コンテンツデータであるKc(Content)と、コンテンツキーK

cをユーザ機器認証サーバ(DAS: Device Authentication Server)の公開鍵:KpDASで暗号化した暗号化コンテンツキーKpDAS(Kc)を格納したコンテンツデータベース110を有する。なお、暗号化コンテンツデータであるKc(Content)は、図にも示すように、それぞれコンテンツ識別子であるコンテンツIDが付加され、コンテンツIDに基づいて識別可能な構成を持つ。

【0049】ショップサーバ100は、さらにコンテンツ取り引き管理データ、例えばコンテンツ販売先のユーザ機器の識別子とコンテンツ識別子等を対応づけて管理する購買管理データベース120を有する。さらに、コンテンツデータベース110からの配信コンテンツの抽出処理、取り引きに伴う購買管理データベース120に対して登録する取り引きデータの生成処理、ユーザ機器200、ユーザ機器認証サーバ300との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段130を有する。

【0050】購買管理データベース120のデータ構成を図3に示す。購買管理データベース120は、ショップサーバがコンテンツ取り引きに応じて処理を実行する際に内部生成する識別番号としてのショップ処理No.、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ID、ユーザ機器とショップ間でのコンテンツ取り引きを実行する際に、ユーザ機器で生成発行するコンテンツ取り引き識別子としてのトランザクションID、取り引き対象コンテンツの識別子であるコンテンツID、ショップサーバにおけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【0051】制御手段130は、図2に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段130は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段130の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ショップサーバ100が格納する暗号鍵等の暗号処理用データとしては、ショップサーバの秘密鍵:KsSHOP、ショップサーバの公開鍵証明書Cert_SHOP、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局(CA: Certificate Authority)の公開鍵KpCAがある。

【0052】図4に制御手段130の構成例を示す。制御手段130の構成について説明する。制御部131は各種処理プログラムを実行する中央演算処理装置(CPU: Central Processing Unit)によって構成され、図4の制御手段の各構成部位の処理を制御する。ROM(Read only Memory)132は、IPL(Initial Program

Loading)等のプログラムを記憶したメモリである。RAM(Random Access Memory)133は、制御部131が実行するプログラム、例えばデータベース管理プログラム、暗号処理プログラム、通信プログラム等、実行プログラムの格納領域、またこれら各プログラム処理におけるワークエリアとして使用される。

【0053】表示部134は、液晶表示装置、CRTなどの表示手段を有し、制御部131の制御の下、様々なプログラム実行時のデータ、例えばコンテンツ配信先のユーザデータ等を表示する。入力部135は、キーボードや、例えばマウス等のポインティングデバイスを有し、これら各入力デバイスからのコマンド、データ入力を制御部131に出力する。HDD(Hard Disk Drive)136は、データベース管理プログラム、暗号処理プログラム、通信プログラム等のプログラム、さらに各種データが格納される。

【0054】ドライブ137は、例えばHD(Hard Disk)や、FD(Floppy Disk)等の磁気ディスク、CD-ROM(Compact Disk ROM)などの光ディスク、ミニディスク等の光磁気ディスク、ROMやフラッシュメモリなどの半導体メモリ等の各種記録媒体に対するアクセスを制御する機能を持つ。磁気ディスク等の各種記録媒体はプログラム、データ等を記憶する。ネットワークインタフェース138は、インターネット、電話回線等の有線、無線を介した通信のインタフェースとして機能する。

【0055】ショップサーバ100は、例えば上述した構成を持つ制御手段130において、コンテンツの取り引き対象であるユーザ機器200、あるいはユーザ機器認証サーバ300との間でのコンテンツ取り引きに伴う様々な暗号処理、認証処理等を実行する。

【0056】(ユーザ機器認証サーバ)図5にユーザ機器認証サーバ(DAS)300の構成を示す。ユーザ機器認証サーバは、ライセンス管理データベース320を有する。ライセンス管理データベース320のデータ構成を図6に示す。ライセンス管理データベースは、コンテンツ取り引き時にユーザ機器認証サーバ(DAS)の実行する処理に応じて内部生成する処理識別子としてのユーザ機器認証サーバ処理No.、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ID、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するコンテンツ取り引き識別子としてのトランザクションID、取り引き対象コンテンツの識別子であるコンテンツID、コンテンツ取り引きを実行するショップサーバの識別子であるショップID、ショップの発行するショップでの処理識別子であるショップ処理No.、ユーザ機器認証サーバ(DAS)におけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される

【0057】ユーザ機器認証サーバ(DAS)300は、ユーザ機器200、ショップサーバ100との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段330を有する。制御手段330は、先に説明したショップサーバの制御手段と同様、暗号処理手段、通信処理手段としての機能も有する。その構成は、図4を用いて説明した構成と同様である。制御手段330の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ユーザ機器認証サーバ(DAS)300が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器認証サーバ(DAS)の秘密鍵:KsDAS、ユーザ機器認証サーバ(DAS)の公開鍵証明書Cert_DAS、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局(CA:Certificate Authority)の公開鍵KpCAがある。

【0058】(ユーザ機器)図7にユーザ機器200の構成を示す。ユーザ機器は、コンテンツの購入を実行し、購入したコンテンツの利用、すなわちコンテンツ再生、実行を行なう例えばコンテンツ再生機器であり、購入管理データベース220を有する。購入管理データベース220のデータ構成を図8に示す。購入管理データベースは、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するコンテンツ取り引き識別子としてのトランザクションID、取り引き対象コンテンツの識別子であるコンテンツID、コンテンツ取り引きを実行するショップサーバの識別子であるショップID、ユーザ機器におけるコンテンツ取り引き処理のステータスを示すステータスの各情報、さらに、ユーザ機器の機器識別子である機器IDを持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【0059】ユーザ機器200は、ショップサーバ100、ユーザ機器認証サーバ300との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段230を有する。制御手段230は、先に説明したショップサーバの制御手段と同様、暗号処理手段、通信処理手段としての機能も有する。その構成は、図4を用いて説明した構成と同様である。制御手段230の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ユーザ機器200が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器の秘密鍵:KsDEV、ユーザ機器の公開鍵証明書Cert_DEV、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局(CA:Certificate Authority)の公開鍵KpCA、コンテンツをユーザ機器の例えばハードディスク等の記憶手段に格納する際の暗号化鍵として適用する保存鍵Kstoがある。

【0060】[公開鍵証明書] 上記ショップサーバ(S

HOP) 100、ユーザ機器 (DEVICE) 200、ユーザ機器認証サーバ (DAS: Device Authentication Server) 300の保有する公開鍵証明書について図9を用いて説明する。

【0061】公開鍵証明書は、公開鍵を用いた暗号データの送受信、あるいはデータ送受信を行なう2者間での相互認証等の処理において、使用する公開鍵が正当な利用者の有する公開鍵であることを第三者、すなわち発行局 (CA: Certificate Authority) が証明したものである。公開鍵証明書のフォーマットの概略を図9(a)に示す。

【0062】バージョン (version) は、証明書フォーマットのバージョンを示す。証明書の通し番号は、シリアルナンバ (Serial Number) であり、公開鍵証明書発行局 (CA) によって設定される公開鍵証明書のシリアルナンバである。署名アルゴリズム識別子、アルゴリズムパラメータ (Signature algorithm Identifier algorithm parameter) は、公開鍵証明書の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびRSAがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、RSAが適用されている場合には鍵長が記録される。発行局の名前は、公開鍵証明書の発行者、すなわち公開鍵証明書発行局 (CA) の名称が識別可能な形式 (Distinguished Name) で記録されるフィールドである。証明書の有効期限 (validity) は、証明書の有効期限である開始日時、終了日時が記録される。公開鍵証明書の利用者名 (ID) は、ユーザである認証対象者の名前が記録される。具体的には例えばユーザ機器のIDや、サービス提供主体のID等である。利用者公開鍵 (subject Public Key Info algorithm subject Public key) は、ユーザの公開鍵情報としての鍵アルゴリズム、鍵情報そのものを格納するフィールドである。発行局が付ける署名は、公開鍵証明書発行局 (CA) の秘密鍵を用いて公開鍵証明書のデータに対して実行される電子署名であり、公開鍵証明書の利用者は、公開鍵証明書発行局 (CA) の公開鍵を用いて検証を行ない、公開鍵証明書の改竄有無がチェック可能となっている。

【0063】公開鍵暗号方式を用いた電子署名の生成方法について、図10を用いて説明する。図10に示す処理は、ECDSA (Elliptic Curve Digital Signature Algorithm)、IEEE P1363/D3) を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号 (Elliptic Curve Cryptography (以下、ECCと呼ぶ)) を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばRSA暗号 (Rivest, Shamir, Adleman) など (ANSI X9.31) を用いることも可能である。

【0064】図10の各ステップについて説明する。ステップS1において、 p を標数、 a, b を楕円曲線の係数 (楕円曲線: $4a^3 + 27b^2 \neq 0 \pmod{p}$)、 G を楕円曲線上のベースポイント、 r を G の位数、 K_s を秘密鍵 ($0 < K_s < r$) とする。ステップS2において、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。

【0065】ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値 (出力) から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、DES-CBCが用いられる場合もある。この場合は、最終出力値となるMAC (チェック値: ICVに相当する) がハッシュ値となる。

【0066】続けて、ステップS3で、乱数 u ($0 < u < r$) を生成し、ステップS4でベースポイントを u 倍した座標 $V(X_v, Y_v)$ を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

【0067】

【数1】 $P=(X_a, Y_a), Q=(X_b, Y_b), R=(X_c, Y_c)=P+Q$ とすると、

$P \neq Q$ の時 (加算)、

$$X_c = \lambda^2 - X_a - X_b$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (Y_b - Y_a) / (X_b - X_a)$$

$P = Q$ の時 (2倍算)、

$$X_c = \lambda^2 - 2X_a$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (3(X_a)^2 + a) / (2Y_a)$$

【0068】これらを用いて点 G の u 倍を計算する (速度は遅いが、最もわかりやすい演算方法として次のように行う。 $G, 2 \times G, 4 \times G, \dots$ を計算し、 u を2進数展開して1が立っているところに対応する $2^i \times G$ (G を i 回2倍算した値 (i は u のLSBから数えた時のビット位置)) を加算する。

【0069】ステップS5で、 $c = X_v \bmod r$ を計算し、ステップS6でこの値が0になるかどうか判定し、0でなければステップS7で $d = [(f + cK_s) / u] \bmod r$ を計算し、ステップS8で d が0であるかどうか判定し、 d が0でなければ、ステップS9で c および d を電子署名データとして出力する。仮に、 r を160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。

【0070】ステップS6において、 c が0であった場合、ステップS3に戻って新たな乱数を生成し直す。同

様に、ステップS8でdが0であった場合も、ステップS3に戻って乱数を生成し直す。

【0071】次に、公開鍵暗号方式を用いた電子署名の検証方法を、図11を用いて説明する。ステップS11で、Mをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、Gを楕円曲線上のベースポイント、rをGの位数、Gおよび $K_s \times G$ を公開鍵（ $0 < K_s < r$ ）とする。ステップS12で電子署名データcおよびdが $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップS13で、メッセージMのハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。次に、ステップS14で $h1 = d \bmod r$ を計算し、ステップS15で $h1 = f \cdot h \bmod r$ 、 $h2 = c \cdot h \bmod r$ を計算する。

【0072】ステップS16において、既に計算したh1およびh2を用い、点 $P = (X_p, Y_p) = h1 \times G + h2 \cdot K_s \times G$ を計算する。電子署名検証者は、公開鍵Gおよび $K_s \times G$ を知っているため、図10のステップS4と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップS17で点Pが無限遠点かどうか判定し、無限遠点でなければステップS18に進む（実際には、無限遠点の判定はステップS16でできてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、λが計算できず、 $P + Q$ が無限遠点であることが判明している）。ステップS18で $X_p \bmod r$ を計算し、電子署名データcと比較する。最後に、この値が一致していた場合、ステップS19に進み、電子署名が正しいと判定する。

【0073】電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【0074】ステップS12において、電子署名データcまたはdが、 $0 < c < r$ 、 $0 < d < r$ を満たさなかった場合、ステップS20に進む。また、ステップS17において、点Pが無限遠点であった場合もステップS20に進む。さらにまた、ステップS18において、 $X_p \bmod r$ の値が、電子署名データcと一致していなかった場合にもステップS20に進む。

【0075】ステップS20において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

【0076】公開鍵証明書には、発行局の署名がなされ、公開鍵利用者による署名検証により、証明書の改竄がチェック可能な構成となっている。図9に戻り説明をつづける。図9（b）がユーザ機器に格納されるユーザ機器の公開鍵証明書：Cert_DEVであり、ユーザ機器IDと、ユーザ機器の公開鍵 $K_p \text{ DEV}$ を格納している。図9（c）はショップサーバに格納されるショップサーバの公開鍵証明書：Cert_SHOPであり、

ショップIDと、ショップサーバの公開鍵 $K_p \text{ SHOP}$ を格納している。図9（d）はユーザ機器認証サーバに格納されるユーザ機器認証サーバの公開鍵証明書：Cert_DASであり、ユーザ機器認証サーバIDと、ユーザ機器認証サーバの公開鍵 $K_p \text{ DAS}$ を格納している。このように、ユーザ機器、ショップサーバ、ユーザ機器認証サーバがそれぞれ公開鍵証明書を保有する。

【0077】【コンテンツ購入処理】次に、図1に戻り、ユーザ機器が、ショップサーバからコンテンツを購入して利用する処理について説明する。図1の番号

（1）から（20）の順に処理が進行する。各番号順に処理の詳細を説明する。なお、本実施例ではエンティティ間の通信において相互認証処理（（1）、（7）、（11））を行なったものを述べているが、必要に応じて省略しても構わない。

【0078】（1）相互認証
コンテンツをショップサーバ100から購入しようとするユーザ機器200は、ショップサーバとの間で相互認証処理を行なう。データ送受信を実行する2つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が1つの好ましいデータ転送方式である。

【0079】共通鍵暗号方式を用いた相互認証方法を、図12を用いて説明する。図12において、共通鍵暗号方式としてDESを用いているが、同様な共通鍵暗号方式であればいずれでもよい。

【0080】まず、Bが64ビットの乱数Rbを生成し、Rbおよび自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数Raを生成し、Ra、Rb、ID(b)の順に、DESのCBCモードで鍵Kabを用いてデータを暗号化し、Bに返送する。

【0081】これを受信したBは、受信データを鍵Kabで復号化する。受信データの復号化方法は、まず、暗号文E1を鍵Kabで復号化し、乱数Raを得る。次に、暗号文E2を鍵Kabで復号化し、その結果とE1を排他的論理和し、Rbを得る。最後に、暗号文E3を鍵Kabで復号化し、その結果とE2を排他的論理和し、ID(b)を得る。こうして得られたRa、Rb、ID(b)の内、RbおよびID(b)が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。

【0082】次にBは、認証後に使用するセッション鍵（Session Key（以下、Ksesとする））を生成する（生成方法は、乱数を用いる）。そして、Rb、Ra、Ksesの順に、DESのCBCモードで鍵Kabを用

いて暗号化し、Aに返送する。

【0083】これを受信したAは、受信データを鍵 K_a bで復号化する。受信データの復号化方法は、Bの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた R_b 、 R_a 、 K_{ses} の内、 R_b および R_a が、Aが送信したものと一致するか検証する。この検証に通った場合、AはBを正当なものとして認証する。互いに相手を認証した後には、セッション鍵 K_{ses} は、認証後の秘密通信のための共通鍵として利用される。

【0084】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0085】次に、公開鍵暗号方式である160ビット長の楕円曲線暗号を用いた相互認証方法を、図13を用いて説明する。図13において、公開鍵暗号方式としてECCを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図13において、まずBが、64ビットの乱数 R_b を生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数 R_a および標数 p より小さい乱数 A_k を生成する。そして、ベースポイント G を A_k 倍した点 $A_v = A_k \times G$ を求め、 R_a 、 R_b 、 A_v （X座標とY座標）に対する電子署名 A_{Sig} を生成し、Aの公開鍵証明書とともにBに返送する。ここで、 R_a および R_b はそれぞれ64ビット、 A_v のX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。

【0086】公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書発行局（CA）410の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局（CA）の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図11で説明したのでその詳細は省略する。

【0087】Aの公開鍵証明書、 R_a 、 R_b 、 A_v 、電子署名 A_{Sig} を受信したBは、Aが送信してきた R_b が、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。そして、取り出したAの公開鍵を用い電子署名 A_{Sig} を検証する。電子署名の検証に成功した後、BはAを正当なものとして認証する。

【0088】次に、Bは、標数 p より小さい乱数 B_k を生成する。そして、ベースポイント G を B_k 倍した点 $B_v = B_k \times G$ を求め、 R_b 、 R_a 、 B_v （X座標とY座標）に対する電子署名 B_{Sig} を生成し、Bの公開鍵証明書とともにAに返送する。

【0089】Bの公開鍵証明書、 R_b 、 R_a 、 B_v 、電子署名 B_{Sig} を受信したAは、Bが送信してきた R_a が、Aが生成したものと一致するか検証する。その結果、一致していた場合には、Bの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Bの公開鍵を取り出す。そして、取り出したBの公開鍵を用い電子署名 B_{Sig} を検証する。電子署名の検証に成功した後、AはBを正当なものとして認証する。

【0090】両者が認証に成功した場合には、Bは $B_k \times A_v$ （ B_k は乱数だが、 A_v は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、Aは $A_k \times B_v$ を計算し、これら点のX座標の下位64ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合）。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【0091】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0092】このような相互認証処理において、生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行する。

【0093】（2）トランザクションID、購入要求データ生成、および

（3）購入要求データ送信

上述のショップサーバ100とユーザ機器200間の相互認証が成功すると、ユーザ機器200は、コンテンツの購入要求データを生成する。購入要求データの構成を図14（a）に示す。購入要求データは、コンテンツ購入の要求先であるショップサーバ100の識別子であるショップID、コンテンツ取り引きの識別子として、ユーザ機器200の暗号処理手段が例えば乱数に基づいて生成するトランザクションID、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツIDの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、購入要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ100に送付される。なお、公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ショップ側に送付済みの場合は、必ずしも改めて送付する必要はない。

【0094】（4）受信データ検証

図14（a）に示す購入要求データをユーザ機器200から受信したショップサーバ100は、受信データの検証処理を実行する。検証処理の詳細について図15を用いて説明する。まず、ショップサーバ100は、受信データ中のユーザ機器の公開鍵証明書 $Cert_DEV$ の

検証(S51)を行なう。これは前述したように、公開鍵証明書に含まれる発行局(CA)の署名を検証する処理(図11参照)として実行され、発行局の公開鍵:KpCAを適用して実行される。

【0095】検証がOK、すなわち公開鍵証明書の改竄がないと判定(S52でYes)されると、S53に進む。検証が非成立の場合(S52でNo)は、S57で公開鍵証明書に改竄ありと判定され、その公開鍵証明書を利用した処理が中止される。S53では、公開鍵証明書からユーザ機器の公開鍵:KpDEVが取り出され、ステップS54で公開鍵:KpDEVを用いた購入要求データのユーザ機器署名の検証処理(図11参照)が実行される。検証がOK、すなわち購入要求データの改竄がないと判定(S55でYes)されると、S56に進み受信データが正当なコンテンツ購入要求データであると判定される。検証が非成立の場合(S55でNo)は、S57で購入要求データが改竄ありと判定され、その購入要求データに対する処理が中止される。

【0096】(5)暗号化コンテンツおよび暗号化コンテンツ鍵データ1(ショップ)送信
ショップサーバ100において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定すると、ショップサーバ100は、暗号化コンテンツおよび暗号化コンテンツ鍵データ1(ショップ)をユーザ機器に送信する。これらは、いずれもコンテンツデータベース110に格納されたデータであり、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ:Kc(content)と、コンテンツキー:Kcをユーザ機器認証サーバ(DAS)300の公開鍵で暗号化した暗号化コンテンツ鍵データ:KpDAS(Kc)である。

【0097】暗号化コンテンツ鍵データ1(ショップ)の構成を図14(b)に示す。暗号化コンテンツ鍵データ1(ショップ)は、コンテンツ購入の要求元であるユーザ機器200の識別子であるユーザ機器ID、購入要求データ(図14(a)のユーザ機器公開鍵証明書を除いたデータ)、コンテンツ取り引きに伴いショップサーバ100が生成したショップ処理No.、暗号化コンテンツ鍵データ:KpDAS(Kc)を有し、これらのデータに対するショップサーバ100の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ1(ショップ)には、ショップサーバ100の公開鍵証明書が添付され、ユーザ機器200に送付される。なお、ショップサーバ公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ユーザ機器側に送付済みの場合は、必ずしも改めて送付する必要はない。

【0098】(6)受信データ検証
ショップサーバ100から暗号化コンテンツ:Kc(content)と、図14(b)に示す暗号化コンテンツ鍵データ1(ショップ)を受信したユーザ機器200は、暗

号化コンテンツ鍵データ1(ショップ)の検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器200は、まずショップサーバ100から受領したショップサーバの公開鍵証明書の検証を発行局(CA)の公開鍵KpCAを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵KpSHOPを用いて図14(b)に示す暗号化コンテンツ鍵データ1(ショップ)のショップ署名の検証を実行する。

【0099】(7)相互認証

ユーザ機器200が、ショップサーバ100から暗号化コンテンツ:Kc(content)と暗号化コンテンツ鍵データ1(ショップ)を受信し、暗号化コンテンツ鍵データ1(ショップ)の検証を終えると、ユーザ機器200は、ユーザ機器認証サーバ300にアクセスし、ユーザ機器200と、ユーザ機器認証サーバ300間において相互認証処理を実行する。この処理は、前述のショップサーバ100とユーザ機器200間の相互認証処理と同様の手続きで実行される。

【0100】(8)暗号化コンテンツ鍵データ(ユーザ機器)および暗号化コンテンツ鍵かけかえ要求送信
ユーザ機器200とユーザ機器認証サーバ300との間の相互認証が成立すると、ユーザ機器200は、ユーザ機器認証サーバ300に対して、先にショップサーバ100から受信した暗号化コンテンツ鍵KpDAS(Kc)を含む暗号化コンテンツ鍵データ(ユーザ機器)と、暗号化コンテンツ鍵かけかえ要求を送信する。

【0101】暗号化コンテンツ鍵データ(ユーザ機器)の構成を図14(c)に示す。暗号化コンテンツ鍵データ(ユーザ機器)は、暗号化コンテンツ鍵かけかえ要求の要求先であるユーザ機器認証サーバ300の識別子であるユーザ機器認証サーバID、ショップサーバ100から受領した暗号化コンテンツ鍵データ(図14(b)のショップ公開鍵証明書を除いたデータ)、を有し、これらのデータに対するユーザ機器200の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ(ユーザ機器)には、ショップサーバ100の公開鍵証明書と、ユーザ機器200の公開鍵証明書が添付され、ユーザ機器認証サーバ300に送付される。なお、ユーザ機器認証サーバ300がユーザ機器公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【0102】(9)受信データ検証

ユーザ機器200から暗号化コンテンツ鍵データ(ユーザ機器)および暗号化コンテンツ鍵かけかえ要求(図14(c))を受信したユーザ機器認証サーバ300は、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器認証サーバ300は、まずユーザ機器200から受領したユーザ機器の公開鍵

証明書の検証を発行局 (CA) の公開鍵 K_{pCA} を用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵 K_{pDEV} を用いて、図 14 (a) に示す購入要求データおよび図 14 (c) に示す暗号化コンテンツ鍵データ (ユーザ機器) の電子署名の検証を実行する。さらに、ショップサーバの公開鍵証明書の検証を発行局 (CA) の公開鍵 K_{pCA} を用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵 K_{pSHOP} を用いて図 14 (c) に示す暗号化コンテンツ鍵データ (ユーザ機器) に含まれる (5) 暗号化コンテンツ鍵データ 1 のショップ署名の検証を実行する。

【0103】 (10) 暗号化コンテンツ鍵かけかえ処理、

ユーザ機器認証サーバ 300 において、ユーザ機器 200 から受信した暗号化コンテンツ鍵データ (ユーザ機器) および暗号化コンテンツ鍵かけかえ要求の検証が終了し、正当な鍵かけかえ要求であると判定すると、ユーザ機器認証サーバ 300 は、暗号化コンテンツ鍵データ (ユーザ機器) に含まれる暗号化コンテンツ鍵、すなわち、コンテンツ鍵: K_c をユーザ機器認証サーバ (DAS) 300 の公開鍵 K_{pDAS} で暗号化したデータ: $K_{pDAS}(K_c)$ をユーザ機器認証サーバ 300 の秘密鍵 K_{sDAS} で復号してコンテンツ鍵 K_c を取得し、さらにコンテンツ鍵 K_c をユーザ機器の公開鍵: K_{pDEV} で暗号化した暗号化コンテンツ鍵: $K_{pDEV}(K_c)$ を生成する。すなわち、 $K_{pDAS}(K_c) \rightarrow K_c \rightarrow K_{pDEV}(K_c)$ の鍵かけかえ処理を実行する。

【0104】図 16 にユーザ機器認証サーバ 300 において実行される暗号化コンテンツ鍵かけかえ処理のフローを示す。まず、ユーザ機器認証サーバ 300 は、ユーザ機器 200 から受信した暗号化コンテンツ鍵データ (ユーザ機器) から、ユーザ機器認証サーバ (DAS) 300 の公開鍵 K_{pDAS} で暗号化したコンテンツ鍵データ: $K_{pDAS}(K_c)$ を取り出す (S61)。次に、ユーザ機器認証サーバ 300 の秘密鍵 K_{sDAS} で復号してコンテンツ鍵 K_c を取得 (S62) する。次に、復号により取得したコンテンツ鍵 K_c をユーザ機器の公開鍵: K_{pDEV} で再暗号化して暗号化コンテンツ鍵: $K_{pDEV}(K_c)$ を生成する (S63)。これらの処理が終了すると、ライセンス管理データベース (図 6 参照) のステータスを「鍵かけかえ完了」に設定する。

【0105】 (11) 相互認証

ユーザ機器認証サーバ 300 において、上述の暗号化コンテンツ鍵の鍵かけかえ処理が完了すると、ユーザ機器認証サーバ 300 は、ショップサーバ 100 にアクセスし、ユーザ機器認証サーバ 300 とショップサーバ 100 間において相互認証処理を実行する。この処理は、前述のショップサーバ 100 とユーザ機器 200 間の相互認証処理と同様の手続きで実行される。

【0106】 (12) 暗号化コンテンツデータ送信

ユーザ機器認証サーバ 300 とショップサーバ 100 間の相互認証が成立すると、ユーザ機器認証サーバ 300 は、暗号化コンテンツ鍵データ (DAS) をショップサーバ 100 に送信する。

【0107】暗号化コンテンツ鍵データ (DAS) の構成を図 17 (d) に示す。暗号化コンテンツ鍵データ

(DAS) は、コンテンツ購入の要求先であるショップサーバ 100 の識別子であるショップ ID、暗号化コンテンツ鍵データ (ユーザ機器) (図 14 (c) のショップおよびユーザ機器公開鍵証明書を除いたデータ)、さらに、前述の鍵かけかえ処理により、ユーザ機器認証サーバ 300 が生成した暗号化コンテンツ鍵データ: $K_{pDEV}(K_c)$ を有し、これらのデータに対するユーザ機器認証サーバ 300 の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ (DAS) には、ユーザ機器認証サーバ 300 と、ユーザ機器 200 の公開鍵証明書が添付され、ショップサーバ 100 に送付される。なお、ショップサーバが、これらの公開鍵証明書を既に保有済みである場合は、必ずしも改めて送付する必要はない。

【0108】また、ユーザ機器認証サーバ 300 が信頼できる第三者機関であると認められる存在である場合は、暗号化コンテンツ鍵データ (DAS) は、図 17

(d) に示すようにユーザ機器の生成した (8) 暗号化コンテンツ鍵データ (ユーザ機器) をそのまま含むデータ構成とすることなく、図 18 (d') に示すように、ユーザ機器 ID、トランザクション ID、コンテンツ ID、ショップ処理 NO、ユーザデバイスの公開鍵で暗号化したコンテンツ鍵 $K_{pDEV}(K_c)$ の各データを、ユーザ機器認証サーバ 300 が抽出して、これらに署名を付加して暗号化コンテンツ鍵データ (DAS) としてもよい。この場合は、(8) 暗号化コンテンツ鍵データ (ユーザ機器) の検証が不要となるので、添付する公開鍵証明書は、ユーザ機器認証サーバ 300 の公開鍵証明書のみでよい。

【0109】 (13) 受信データ検証

ユーザ機器認証サーバ 300 から暗号化コンテンツ鍵データ (DAS) (図 17 (d)) を受信したショップサーバ 100 は、暗号化コンテンツ鍵データ (DAS) の検証処理を実行する。この検証処理は、先に説明した図 15 の処理フローと同様の処理であり、ショップサーバ 100 は、まずユーザ機器認証サーバ 300 から受領したユーザ機器認証サーバの公開鍵証明書の検証を発行局 (CA) の公開鍵 K_{pCA} を用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ 300 の公開鍵 K_{pDAS} を用いて図 17 (d) に示す暗号化コンテンツ鍵データ (DAS) の電子署名の検証を実行する。さらに、ユーザ機器の公開鍵証明書の検証を発行局 (CA) の公開鍵 K_{pCA} を用いて実行し、次に公開鍵

証明書から取り出したユーザ機器の公開鍵KpDEVを用いて図17(d)に示す暗号化コンテンツ鍵データ(DAS)に含まれる(8)暗号化コンテンツ鍵データ(ユーザ機器)のユーザ機器署名の検証を実行する。さらに、また、自己の公開鍵KpSHOPを用いて、暗号化コンテンツデータ(ユーザ機器)を検証するようにしてもよい。

【0110】なお、先に説明した図18(d')の簡略化した暗号化コンテンツ鍵データ(DAS)をショップサーバ100が受領した場合は、ショップサーバ100は、ユーザ機器認証サーバの公開鍵証明書の検証を発行局(CA)の公開鍵KpCAを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ300の公開鍵KpDASを用いて図18(d')に示す暗号化コンテンツ鍵データ(DAS)の電子署名の検証を実行するのみの処理となる。

【0111】(14)相互認証、および

(15)暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器200は、暗号化コンテンツ鍵要求データをショップサーバ100に対して送信する。なお、この際、前の要求と異なるセッションで要求を実行する場合は、再度相互認証を実行して、相互認証が成立したことを条件として暗号化コンテンツ鍵要求データがユーザ機器200からショップサーバ100に送信される。

【0112】暗号化コンテンツ鍵要求データの構成を図17(e)に示す。暗号化コンテンツ鍵要求データは、コンテンツ購入の要求先であるショップサーバ100の識別子であるショップID、先にユーザ機器200が生成したコンテンツ取り引きの識別子であるトランザクションID、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツID、さらに、先にショップが生成し暗号化コンテンツ鍵データ1(ショップ)としてユーザ機器200に送信してきたデータ(図14(b)参照)中に含まれるショップ処理No.を有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、暗号化コンテンツ鍵要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ100に送付される。なお、公開鍵証明書が既にショップ側に保管済みの場合は、必ずしも改めて送付する必要はない。

【0113】(16)検証処理、および

(17)課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ100は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、図15を用いて説明したと同様の処理である。データ検証が済むと、ショップサーバ100は、コンテンツの取り引きに関する課金処理を実行する。課金処理は、ユーザの取り引き口座からコンテンツ料金を受領する処理である。受領したコンテンツ料金は、コンテンツの著作権者、ショップ、ユ

ーザ機器認証サーバ管理者など、様々な関係者に配分される。

【0114】この課金処理に至るまでには、ユーザ機器認証サーバ300による暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となっているので、ショップサーバ100は、ユーザ機器間とのみの処理では課金処理が実行できない。また、ユーザ機器200においても暗号化コンテンツ鍵の復号ができないので、コンテンツの利用ができない。ユーザ機器認証サーバは、図6を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべての課金対象となるコンテンツ取り引きが把握可能となる。従って、ショップ側単独でのコンテンツ取り引きは不可能となり、不正なコンテンツ販売が防止される。

【0115】(18)暗号化コンテンツ鍵データ2(ショップ)送信

ショップサーバ100における課金処理が終了すると、ショップサーバ100は、暗号化コンテンツ鍵データ2(ショップ)をユーザ機器200に送信する。

【0116】暗号化コンテンツ鍵データ2(ショップ)の構成を図17(f)に示す。暗号化コンテンツ鍵データ2(ショップ)は、暗号化コンテンツ鍵要求の要求元であるユーザ機器200の識別子であるユーザ機器ID、ユーザ機器認証サーバ300から受領した暗号化コンテンツ鍵データ(DAS)(図17(d)のユーザ機器、ユーザ機器認証サーバ公開鍵証明書を除いたデータ)、を有し、これらのデータに対するショップサーバ100の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ2(ショップ)には、ショップサーバ100の公開鍵証明書と、ユーザ機器認証サーバ300の公開鍵証明書が添付され、ユーザ機器200に送付される。なお、ユーザ機器200がユーザ機器認証サーバ公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【0117】なお、ユーザ機器認証サーバ300が信頼できる第三者機関であると認められる存在であり、ショップサーバ100がユーザ機器認証サーバ300から受信する暗号化コンテンツ鍵データ(DAS)が先に説明した図18(d')の簡略化した暗号化コンテンツ鍵データ(DAS)である場合は、ショップサーバ100は、図18(f')に示す暗号化コンテンツ鍵データ2(ショップ)をユーザ機器に送付する。すなわち、図18(d')に示す簡略化した暗号化コンテンツ鍵データ(DAS)にショップサーバの署名を付加したデータに、ショップサーバ100の公開鍵証明書と、ユーザ機器認証サーバ300の公開鍵証明書を添付してユーザ機器200に送付する。

【0118】(19)受信データ検証

ショップサーバ100から、暗号化コンテンツ鍵データ2(ショップ)を受領したユーザ機器200は、暗号化コンテンツ鍵データ2(ショップ)の検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器200は、まずショップサーバ100から受領したショップサーバの公開鍵証明書の検証を発行局(CA)の公開鍵K_pCAを用いて実行し、次に公開鍵証明書から取り出したショップサーバ100の公開鍵K_pSHOPを用いて図17(f)に示す暗号化コンテンツ鍵データ2(ショップ)の電子署名の検証を実行する。さらに、ユーザ機器認証サーバ300の公開鍵証明書の検証を発行局(CA)の公開鍵K_pCAを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ300の公開鍵K_pDASを用いて図17(f)に示す暗号化コンテンツ鍵データ2(ショップ)に含まれる(12)暗号化コンテンツ鍵データ(DAS)の署名検証を実行する。さらにまた、自己の公開鍵K_pDEVを用いて、暗号化コンテンツデータ(ユーザ機器)を検証するようにしてもよい。

【0119】(20)保存処理

ショップサーバ100から受信した暗号化コンテンツ鍵データ2(ショップ)を検証したユーザ機器200は、暗号化コンテンツ鍵データ2(ショップ)に含まれる自己の公開鍵K_pDEVで暗号化された暗号化コンテンツ鍵:K_pDEV(K_c)を自己の秘密鍵K_sDEVを用いて復号し、さらに、ユーザ機器の保存鍵K_stoを用いて暗号化して暗号化コンテンツ鍵:K_sto(K_c)を生成して、これをユーザ機器200の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵:K_sto(K_c)を保存鍵K_stoを用いて復号してコンテンツ鍵K_cを取り出して、取り出したコンテンツ鍵K_cを用いて、暗号化コンテンツK_c(Content)の復号処理を実行し、コンテンツ(Content)を再生、実行する。

【0120】ユーザ機器200におけるコンテンツ鍵K_cの取得と保存処理フローを図19に示す。ユーザ機器200は、まず、ショップサーバ100から受信した暗号化コンテンツ鍵データ2(ショップ)から自己の公開鍵K_pDEVで暗号化された暗号化コンテンツ鍵:K_pDEV(K_c)を取り出し(S71)、取り出した暗号化コンテンツ鍵:K_pDEV(K_c)を自己の秘密鍵K_sDEVを用いて復号してコンテンツ鍵K_cを取り出す(S72)。さらに、ユーザ機器の保存鍵K_stoを用いてコンテンツ鍵K_cの暗号化処理を実行して暗号化コンテンツ鍵:K_sto(K_c)を生成して、これをユーザ機器200の記憶手段(内部メモリ)に格納(S73)する。

【0121】以上の処理により、ユーザ機器は、暗号化コンテンツK_c(Content)と、該暗号化コンテンツのコンテンツ鍵K_cを取得することができ、コンテンツを

利用することができる。上述の説明から明らかなように、ユーザ機器200においてコンテンツ利用可能な状態に至るまでには、ユーザ機器認証サーバ300における暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須である。従って、ショップサーバ100は、ユーザ機器200に対して、ユーザ機器認証サーバ300に秘密にコンテンツを販売し、コンテンツをユーザ機器において利用可能な状態とすることができない。ユーザ機器認証サーバは、図6を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべてのショップの取り引きの管理がなされ、課金されたコンテンツ取り引きを把握し、ショップの課金処理において受領されたコンテンツ料金を、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に正確に配分することが可能となる。

【0122】(各機器におけるステータス遷移)図1に示すショップサーバ100、ユーザ機器200、ユーザ認証サーバ(DAS)300は、それぞれコンテンツ取り引きに係る一連の処理において、処理状態を示すステータスに応じて、次の処理を決定する。ステータスは、例えば図3に示すショップサーバの購買管理データベース、図6のユーザ機器認証サーバのライセンス管理データベース、図8のユーザ機器の購入管理データベースにおいて、各コンテンツ取り引き毎に管理される。

【0123】まず、ショップサーバ100のステータス遷移について、図20を用いて説明する。ショップサーバは、ユーザ機器200からのコンテンツ購入要求データを受信(図1の処理(3)に対応)することで処理が開始される。ショップサーバ100は、ユーザ機器200からの受信データを検証し、検証に成功した場合は、ステータスを「購入受付完了」に設定し、データ検証により正当な購入要求であるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、購入受付処理を所定回数繰り返した後処理を中止し、ステータスを「購入受付失敗」とする。ステータスが「購入受付完了」である場合にのみ次ステップに進む。

【0124】ステータスが「購入受付完了」に遷移すると、次に、ショップサーバ100は、ユーザ機器200に対して暗号化コンテンツ鍵データ1(ショップ)を送信(図1の処理(5)に対応)し、ユーザ機器からの受信応答(レスポンス)を受領することにより、ステータスを「鍵1配信完了」とする。鍵データ1の送信が成功しなかった場合は、処理を中止するか、あるいは同様の処理、ここでは、鍵データ1の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵1配信失敗」とする。ステータスが「鍵1配信完了」である場合にのみ次ステップに進む。

【0125】ステータスが「鍵1配信完了」に遷移した

場合、次に、ショップサーバ100は、ユーザ機器認証サーバ300から暗号化コンテンツ鍵データ(DAS)を受信(図1の処理(12)に対応)し、データ検証を実行する。検証に成功した場合は、ステータスを「鍵受信完了」に設定し、データ検証により正当な暗号化コンテンツ鍵データ(DAS)であるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵受信失敗」とする。ステータスが「鍵受信完了」である場合にのみ次ステップに進む。

【0126】ステータスが「鍵受信完了」に遷移した場合、次に、ショップサーバ100は、ユーザ機器200から暗号化コンテンツ鍵送信要求データを受信(図1の処理(15)に対応)し、データ検証を実行する。検証に成功した場合は、ステータスを「暗号化コンテンツ鍵送信要求受付完了」に設定し、データ検証により正当な鍵送信要求データであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵送信要求データの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「暗号化コンテンツ鍵送信要求受付失敗」とする。ステータスが「暗号化コンテンツ鍵送信要求受付完了」である場合にのみ次ステップに進む。

【0127】ステータスが「暗号化コンテンツ鍵送信要求受付完了」に遷移した場合、次に、ショップサーバ100は、課金処理(図1の処理(17)に対応)を実行する。課金処理が完了すると、ステータスを「課金完了」に設定し、課金処理が終了しなかった場合、例えばユーザ機器の指定口座からのコンテンツ料金引き落としができなかった場合などには、以降の処理は実行せず、処理を中止するか、あるいは同様の処理、ここでは、課金処理を所定回数繰り返した後、処理を中止し、ステータスを「課金失敗」とする。ステータスが「課金完了」である場合にのみ次ステップに進む。

【0128】ステータスが「課金完了」に遷移した場合、次に、ショップサーバ100は、ユーザ機器へ暗号化コンテンツ鍵データ2(ショップ)送信処理(図1の処理(18)に対応)を実行する。暗号化コンテンツ鍵データ2(ショップ)送信処理が完了し、ユーザ機器からの受信レスポンスを受信すると、ステータスを「鍵2配信完了」に設定し、鍵データ2(ショップ)送信処理が終了しなかった場合には、ステータスを「鍵2配信失敗」とする。ステータスが「鍵2配信完了」である場合にのみ次ステップ、ここでは処理終了となり、ステータスが「鍵2配信失敗」である場合は、以降の処理は実行せず、処理を中止するか、あるいは同様の処理、ここでは、鍵データ2(ショップ)送信処理を所定回数繰り返す。ショップサーバ100は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【0129】次に、ユーザ機器200のステータス遷移について、図21を用いて説明する。ユーザ機器200は、まず、ショップサーバ100に対してコンテンツ購入要求データを送信(図1の処理(3)に対応)することで処理が開始される。ユーザ機器200は、ショップサーバ100に対するコンテンツ購入要求データの受信完了のレスポンスを受信すると、ステータスを「購入要求送信完了」に設定し、ショップサーバ100からの受信完了のレスポンスを受信できない場合は、処理を中止するか、あるいは同様の処理、ここでは、購入要求送信処理を所定回数繰り返した後、処理を中止し、ステータスを「購入要求送信失敗」とする。ステータスが「購入要求送信完了」である場合にのみ次ステップに進む。

【0130】ステータスが「購入要求送信完了」に遷移すると、次に、ユーザ機器200は、ショップサーバ100から、暗号化コンテンツ鍵データ1(ショップ)を受信(図1の処理(5)に対応)し、受信データを検証する。ショップサーバ100からの暗号化コンテンツ鍵データの検証に成功した場合は、ステータスを「鍵1受信完了」に設定し、データ検証により正当な暗号化コンテンツ鍵データであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵1受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵1受信失敗」とする。ステータスが「鍵1受信完了」である場合にのみ次ステップに進む。

【0131】ステータスが「鍵1受信完了」に遷移した場合、次に、ユーザ機器200は、ユーザ機器認証サーバ300に対して、暗号化コンテンツ鍵データ(ユーザ機器)を送信(図1の処理(8)に対応)し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「鍵送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、鍵送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵送信失敗」とする。ステータスが「鍵送信完了」である場合にのみ次ステップに進む。

【0132】ステータスが「鍵送信完了」に遷移した場合、次に、ユーザ機器200は、ショップサーバ100に対して、暗号化コンテンツ鍵送信要求を送信(図1の処理(15)に対応)し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「暗号化コンテンツ鍵送信要求送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵送信要求送信処理を所定回数繰り返した後、処理を中止し、ステータスを「暗号化コンテンツ鍵送信要求送信失敗」とする。ステータスが「暗号化コンテンツ鍵送信要求送信完了」である場合にのみ次ステップに進む。

【0133】ステータスが「暗号化コンテンツ鍵送信要求送信完了」に遷移した場合、次に、ユーザ機器200は、ショップサーバ100から、暗号化コンテンツ鍵データ2（ショップ）を受信（図1の処理（18）に対応）し、データ検証を行なう。データ検証に成功した場合は、ステータスを「鍵2受信完了」に設定し、データ検証に成功しなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵データ2（ショップ）受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵2受信失敗」とする。ステータスが「鍵2受信完了」である場合には処理終了となる。ユーザ機器200は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【0134】次にユーザ機器認証サーバ300のステータス遷移について、図22を用いて説明する。ユーザ機器認証サーバ300は、ユーザ機器200からの暗号化コンテンツ鍵データ（ユーザ機器）を受信（図1の処理（8）に対応）することで処理が開始される。ユーザ機器認証サーバ300は、ユーザ機器200からの受信データを検証し、検証に成功した場合は、ステータスを「鍵受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（ユーザ機器）の受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵受信失敗」とする。ステータスが「鍵受信完了」である場合にはのみ次ステップに進む。

【0135】ステータスが「鍵受信完了」に遷移すると、次に、ユーザ機器認証サーバ300は、コンテンツ鍵かけかえ処理（図1の処理（10）に対応）を実行し、鍵かけかえ処理が完了した場合には、ステータスを「鍵かけかえ完了」とする。鍵かけかえに失敗することは想定していないので、ここでは「鍵かけかえ完了」のみのステータス遷移が存在する。

【0136】ステータスが「鍵かけかえ完了」に遷移した場合、次に、ユーザ機器認証サーバ300は、ショップサーバ100に対して暗号化コンテンツ鍵データ（DAS）を送信（図1の処理（12）に対応）し、ショップサーバ100からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「鍵送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（DAS）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵送信失敗」とする。ステータスが「鍵送信完了」である場合には、処理終了となる。ユーザ機器認証サーバ300は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【0137】（コンテンツ購入処理フロー）次に、ユーザ機器からショップサーバに対するコンテンツ購入要求

に伴ってショップサーバ100、ユーザ機器200、ユーザ機器認証サーバ300間で実行されるデータ送受信処理をフローに従って説明する。処理フローは、以下のA、B、C、Dに分割して説明する。

【0138】A. ショップサーバとユーザ機器間における処理（図1に示す（1）～（6）の処理）
ユーザ機器200とショップサーバ100の相互認証～ユーザ機器200からショップサーバ100に対するコンテンツ購入要求～ショップサーバ100からユーザ機器200に対する鍵1（ショップ）の送信。

B. ユーザ機器認証サーバとユーザ機器間における処理（図1に示す（7）～（9）の処理）

ユーザ機器200とユーザ機器認証サーバ300の相互認証～暗号化コンテンツ鍵データ送信～ユーザ機器認証サーバ300における受信データ検証。C. ユーザ機器認証サーバとショップサーバ間における処理（図1に示す（11）～（13）の処理）

ユーザ機器認証サーバ300とショップサーバ100間の相互認証～暗号化コンテンツ鍵データ（DAS）送信～ショップサーバにおける受信データ検証。D. ショップサーバとユーザ機器間における処理（図1に示す（14）～（19）の処理）

ユーザ機器200とショップサーバ100の相互認証～ユーザ機器200からショップサーバ100に対する暗号化コンテンツ鍵要求データ送信～ショップサーバ100からユーザ機器200に対する鍵2（ショップ）の送信～ユーザ機器200における受信データ検証。

【0139】まず、A. ショップサーバとユーザ機器間における処理（図1に示す（1）～（6）の処理）について、図23、図24を用いて説明する。

【0140】図23、図24において、左側がショップサーバの処理、右側がユーザ機器の処理を示す。なお、すべてのフローにおいて、ショップサーバの処理ステップNoをS10xx、ユーザ機器の処理ステップNoをS20xx、ユーザ機器認証サーバの処理ステップNoをS30xxとして示す。

【0141】まず、図23に示すように、処理開始時に、ショップサーバとユーザ機器間において相互認証が実行される（S1001、S2001）。相互認証処理は、図12または図13を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ショップサーバは、購買管理データベース（図3参照）に新規ショップ処理NOを新たな処理エントリとして追加（S1003）する。

【0142】一方、ユーザ機器は、相互認証が成立すると、今回のコンテンツ取り引きにおいて適用するトランザクションIDを例えば乱数に基づいて生成し、購入データベース（図8参照）に新規トランザクションIDを

新たなエントリとして追加 (S2003) する。さらに、ユーザ機器は、ショップサーバに対するコンテンツ購入要求データの送信 (S2004)、すなわち、図14 (a) に示す (3) 購入要求データの送信を実行する。

【0143】ショップサーバは、ユーザ機器からのコンテンツ購入要求データを受信 (S1004) し、受信データ (S1005) の検証を実行する。データ検証は、先に説明した図11の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器に対して受信OKのレスポンスを送信 (S1008) し、購買管理データベースのステータスを「購入受付完了」に設定 (S1010) する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器に対して受信NGのレスポンスを送信 (S1007) し、購買管理データベースのステータスを「購入受付失敗」に設定 (S1009) する。

【0144】ユーザ機器は、ショップサーバからの受信OKのレスポンスを受信 (S2005、S2006でYes) すると、購入管理データベースのステータスを「購入要求送信完了」に設定し、ショップサーバからの受信NGレスポンスを受信 (S2005、S2006でNo) すると、購入管理データベースのステータスを「購入要求送信失敗」に設定する。

【0145】ショップサーバでは、購買管理データベースのステータスを「購入受付完了」に設定 (S1010) 後、暗号化コンテンツ鍵データ1 (ショップ) (図14 (b) 参照) を生成 (S1011) し、ユーザ機器に対して、コンテンツ鍵: Kc (Content) を送信 (S1012) し、さらに、図14 (b) に示す暗号化コンテンツ鍵データ1 (ショップ) を送信 (S1013) する。

【0146】ユーザ機器は、購入管理データベースのステータスを「購入要求送信完了」に設定 (S2007) 後、ショップサーバから、コンテンツ鍵: Kc で暗号化した暗号化コンテンツ: Kc (Content) を受信 (S2009) し、さらに、ショップサーバから暗号化コンテンツ鍵データ1 (ショップ) (図14 (b)) を受信 (S2010) する。

【0147】ユーザ機器は、ステップS2009、S2010で受信したデータの検証処理 (図11参照) を実行 (S2021) し、受信データの検証により、データが改竄のない正当なデータであると認められると、ショップサーバに対して受信OKのレスポンスを送信 (S2023) し、購入管理データベースのステータスを「鍵1受信完了」に設定 (S2025) する。受信データの検証により、データが改竄のある不当なデータであると認められると、ショップサーバに対して受信NGのレスポンスを送信 (S2024) し、購入管理データベース

のステータスを「鍵1受信失敗」に設定 (S2026) した後、ショップサーバとの接続を切る (S2027)。

【0148】ショップサーバは、ユーザ機器からのレスポンスを受信 (S1021) し、レスポンスがOKである場合は、購買管理データベースのステータスを「鍵1配信成功」に設定 (S1024) する。レスポンスがNGである場合は、購買管理データベースのステータスを「鍵1配信失敗」に設定 (S1023) した後、ユーザ機器との接続を切る (S1025)。

【0149】なお、ステップS1002、S2002の相互認証失敗の場合、S1009のステータスの「購入受付失敗」の設定、および、S2008のステータスの「購入要求送信失敗」の設定の場合は、いずれも処理を中止して、接続を切る処理を行なって処理終了とする。

【0150】次に、B. ユーザ機器認証サーバとユーザ機器間における処理 (図1に示す (7) ~ (9) の処理) について、図25のフローに従って説明する。

【0151】まず、ユーザ機器認証サーバとユーザ機器間において相互認証が実行される (S3001、S2031)。相互認証処理は、図12または図13を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ユーザ機器認証サーバは、ライセンス管理データベース (図6参照) に新規ユーザ機器認証サーバ処理NO、を新たな処理エントリとして追加 (S3003) する。

【0152】一方、ユーザ機器は、相互認証が成立すると、暗号化コンテンツ鍵データ (ユーザ機器) (図14 (c) 参照) を生成 (S2033) し、ユーザ機器認証サーバへ送信 (S2034) する。

【0153】ユーザ機器認証サーバは、ユーザ機器からの暗号化コンテンツ鍵データ (ユーザ機器) を受信 (S3004) し、受信データの検証 (S3005) を実行する。データ検証は、先に説明した図11の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器に対して受信OKのレスポンスを送信 (S3008) し、ライセンス管理データベースのステータスを「鍵受信完了」に設定 (S3010) する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器に対して受信NGのレスポンスを送信 (S3007) し、ライセンス管理データベースのステータスを「鍵受信失敗」に設定 (S3009) 後、ユーザ機器との接続を切る (S3011)。

【0154】ユーザ機器は、ユーザ機器認証サーバからの受信OKのレスポンスを受信 (S2035、S2036でYes) すると、購入管理データベースのステータスを「鍵送信完了」に設定 (S2037) し、ユーザ機

器認証サーバからの受信NGレスポンスを受信（S2035, S2036でNo）すると、購入管理データベースのステータスを「鍵送信失敗」に設定（S2038）した後、ユーザ機器認証サーバとの接続を切る（S2039）。

【0155】なお、ステップS3002, S2032の相互認証失敗の場合は、処理を中止して、接続を切る処理を行なって処理終了とする。

【0156】次に、C. ユーザ機器認証サーバとショップサーバ間における処理（図1に示す（11）～（13）の処理）について、図26のフローに従って説明する。

【0157】まず、ユーザ機器認証サーバとショップサーバ間において相互認証が実行される（S3021, S1031）。相互認証処理は、図12または図13を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ユーザ機器認証サーバは、暗号化コンテンツ鍵データ（DAS）（図17（d）参照）を生成（S3023）し、ショップサーバへ送信（S3024）する。

【0158】一方、ショップサーバは、相互認証の成立後、ユーザ機器認証サーバから暗号化コンテンツ鍵データ（DAS）（図17（d）参照）を受信（S1033）し、受信データの検証（S1034）を実行する。データ検証は、先に説明した図11の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器認証サーバに対して受信OKのレスポンスを送信（S1036）し、購入管理データベースのステータスを「鍵受信完了」に設定（S1038）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器認証サーバに対して受信NGのレスポンスを送信（S1037）し、購入管理データベースのステータスを「鍵受信失敗」に設定（S1039）後、ユーザ機器認証サーバとの接続を切る（S1040）。

【0159】ユーザ機器認証サーバは、ショップサーバからの受信OKのレスポンスを受信（S3025, S3026でYes）すると、ライセンス管理データベースのステータスを「鍵送信完了」に設定（S3028）し、ショップサーバからの受信NGレスポンスを受信（S3025, S3026でNo）すると、ライセンス管理データベースのステータスを「鍵送信失敗」に設定（S3027）した後、ユーザ機器認証サーバとの接続を切る（S3029）。

【0160】なお、ステップS3022, S1032の相互認証失敗の場合は、処理を中止して、接続を切る処理を行なって処理終了とする。

【0161】次に、D. ショップサーバとユーザ機器間における処理（図1に示す（14）～（19）の処理）について、図27、図28を用いて説明する。

【0162】まず、処理開始時に、ショップサーバとユーザ機器間において相互認証が実行される（S1051, S2051）。相互認証処理は、図12または図13を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ユーザ機器は、暗号化コンテンツ鍵送信要求データ（図17（e）参照）を生成（S2053）し、ショップサーバへ送信（S2054）する。

【0163】ショップサーバは、ユーザ機器からの暗号化コンテンツ鍵送信要求データを受信（S1054）し、受信データの検証を実行（S1055）する。データ検証は、先に説明した図11の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器に対して受信OKのレスポンスを送信（S1058）し、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求受付完了」に設定（S1060）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器に対して受信NGのレスポンスを送信（S1057）し、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求受付失敗」に設定（S1059）する。

【0164】ユーザ機器は、ショップサーバからの受信OKのレスポンスを受信（S2055, S2056でYes）すると、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求送信完了」に設定（S2057）し、ショップサーバからの受信NGレスポンスを受信（S2055, S2056でNo）すると、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求送信失敗」に設定（S2058）する。

【0165】ショップサーバでは、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求受付完了」に設定（S1060）後、暗号化コンテンツ鍵データ2（ショップ）（図17（f）参照）を生成（S1061）し、ユーザ機器に対して、図17（f）に示す暗号化コンテンツ鍵データ2（ショップ）を送信（S1062）する。

【0166】ユーザ機器は、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求送信完了」に設定（S2057）後、ショップサーバから、暗号化コンテンツ鍵データ2（ショップ）（図17（f））を受信（S2059）する。

【0167】ユーザ機器は、ステップS2059で受信したデータの検証処理（図11参照）を実行（S2071）し、受信データの検証により、データが改竄のない正当なデータであると認められると、ショップサーバに

対して受信OKのレスポンスを送信（S2073）し、購入管理データベースのステータスを「鍵2受信完了」に設定（S2075）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ショップサーバに対して受信NGのレスポンスを送信（S2074）し、購入管理データベースのステータスを「鍵2受信失敗」に設定（S2076）した後、ショップサーバとの接続を切る（S2077）。

【0168】ショップサーバは、ユーザ機器からのレスポンスを受信（S1071）し、レスポンスがOKである場合は、購入管理データベースのステータスを「鍵2配信成功」に設定（S1074）する。レスポンスがNGである場合は、購入管理データベースのステータスを「鍵2配信失敗」に設定（S1073）した後、ユーザ機器との接続を切る（S1075）。

【0169】なお、ステップS1052、S2052の相互認証失敗の場合は、処理を中止して、接続を切る処理を行なって処理終了とする。

【0170】【基本コンテンツ配信モデル1の変形例】ここまで、図1に示した基本コンテンツ配信モデル1の構成に基づいてコンテンツ購入処理の構成、処理手順について説明してきたが、基本的にユーザ機器認証サーバにおいてコンテンツ鍵のかけかえ処理を実行する構成とするポリシーを持つ構成であれば、図1に示す構成に限らず、様々な態様が実現可能である。以下、様々な変形例について説明する。

【0171】図29に示す構成は、ショップサーバの機能を分離し、ショップサーバと配信サーバを設けた構成である。ショップサーバ100は、ユーザ機器200からのコンテンツ購入要求を受領するが、ユーザ機器200に対するコンテンツ配信は配信サーバ400が実行する。本例では、各エンティティ間で相互認証処理を省略しているが、基本コンテンツ配信モデル1同様、相互認証処理を行なっても構わない。

【0172】ショップサーバ100は、ユーザ機器200からの購入要求データを受信し、データの検証（図29の処理（3））を行なって、要求データの正当性を確認した後、配信サーバ400に対して、コンテンツ配信要求の送信を実行（図29の処理（4））する。配信サーバ400は、ショップサーバ100からのコンテンツ配信要求データを検証し、データの正当性が確認された場合、コンテンツデータベース410から取り出した暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を送信（図29の処理（6））する。暗号化コンテンツ鍵データ（配信サーバ）は、前述の実施例の暗号化コンテンツ鍵データ1（ショップ）に対応し、ユーザ機器認証サーバの公開鍵KpDASで暗号化したコンテンツ鍵Kc、すなわちKpDAS（Kc）を含むデータである。

【0173】ユーザ機器200が配信サーバ400から

暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を受信した後の処理は、先の図1に示した構成に基づく実施例と同様となる。

【0174】本構成においては、ショップサーバ100は、ユーザ機器からのコンテンツ要求を受け付けて、その正当性を検証する機能、ユーザ機器認証サーバからの、かけかえ済みの暗号化コンテンツ鍵を受信し、ユーザ機器に対する配信を主として実行し、コンテンツ自体の管理、配信を行なわない。従って、例えば音楽データを管理する音楽コンテンツ配信サーバ、ゲームコンテンツを管理するゲームコンテンツ配信サーバ等、様々なコンテンツ管理主体となる複数の配信サーバに対して1つのショップサーバがユーザ機器からのコンテンツ要求に応答し、ショップサーバが要求に応じて要求コンテンツを管理する配信サーバにコンテンツ配信要求を送信する構成に適した態様である。また、この構成にしたことにより、例えば、ユーザ機器とショップサーバは双方向通信であるため、インターネットを使うが、配信サーバからユーザ機器へは片方向通信であるため、高速な衛星通信が利用できるメリットがある。

【0175】図30は、図29と同様ショップサーバの機能を分離し、ショップサーバと配信サーバを設けた構成であり、ショップサーバ100は、ユーザ機器200からのコンテンツ購入要求を受領するが、ユーザ機器200に対するコンテンツ配信は配信サーバ400が実行する。図29の構成と異なる点は、ショップサーバ100から配信サーバ400に対してコンテンツ配信要求を送信せず、ユーザ機器認証サーバ300が、配信サーバ400に対してコンテンツ配信要求を送信する構成とした点である。

【0176】ショップサーバ100は、ユーザ機器200からの購入要求データを受信し、データの検証（図30の処理（3））を行なって、要求データの正当性を確認した後、ユーザ機器認証サーバ300に対して、コンテンツ配信要求の送信を実行（図30の処理（4））する。その後、ユーザ機器認証サーバ300は、データの検証（図30の処理（5））を行なって、要求データの正当性を確認した後、配信サーバ400に対して、コンテンツ配信要求の送信を実行（図30の処理（6））する。配信サーバ400は、ユーザ機器認証サーバ300からのコンテンツ配信要求データを検証し、正当性が確認された場合、ユーザ機器200に対して、コンテンツデータベース410から取り出した暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を送信

（図30の処理（8））する。暗号化コンテンツ鍵データ（配信サーバ）は、前述の実施例の暗号化コンテンツ鍵データ1（ショップ）に対応し、ユーザ機器認証サーバの公開鍵KpDASで暗号化したコンテンツ鍵Kc、すなわちKpDAS（Kc）を含むデータである。

【0177】ユーザ機器200が配信サーバ400から

暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を受信した後の処理は、先の図1に示した構成に基づく実施例と同様となる。

【0178】本構成においては、ユーザ機器認証サーバ300は、ユーザ機器200からの鍵のかけかえ要求以前、ショップサーバ100に対してコンテンツ購入要求があった時点で、コンテンツ購入要求主体であるユーザ機器情報を取得し、管理することが可能となる。従って、ユーザ機器200からの鍵のかけかえ要求受領時に、すでに登録済みのコンテンツ購入要求ユーザ機器であるか否かの照合処理が可能となる。

【0179】[1. 3. 基本コンテンツ配信モデル2]次に、図31を用いて基本コンテンツ配信モデル1と異なる基本コンテンツ配信モデル2について説明する。基本コンテンツ配信モデル2では、ユーザ機器200とユーザ機器認証サーバ300の間ではデータ送受信が行われない。図31に示す各処理(1)～(19)について、基本コンテンツ配信モデル1との相違点を中心に説明する。なお、本実施例では、エンティティ間の通信において相互認証処理((1)、(7)、(13))を行なったものを述べているが、必要に応じて省略しても構わない。

【0180】(1) 相互認証

コンテンツをショップサーバ100から購入しようとするユーザ機器200は、ショップサーバ100との間で相互認証処理を行なう。相互認証処理は、図12または図13を用いて説明した処理である。相互認証処理において、生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。

【0181】(2) トランザクションID、購入要求データ生成、および

(3) 購入要求データ送信

ショップサーバ100とユーザ機器200間の相互認証が成功すると、ユーザ機器200は、コンテンツの購入要求データを生成する。購入要求データの構成を図32(g)に示す。購入要求データは、コンテンツ購入の要求先であるショップサーバ100の識別子であるショップID、コンテンツ取り引きの識別子として、ユーザ機器200の暗号処理手段が乱数に基づいて生成するトランザクションID、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツIDの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、購入要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ100に送付される。なお、公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ショップ側に送付済みの場合は、必ずしも改めて送付する必要はない。

【0182】(4) 受信データ検証

図32(g)に示す購入要求データをユーザ機器200

から受信したショップサーバ100は、受信データの検証処理を実行する。検証処理の詳細は、先に図15を用いて説明した通りである。

【0183】(5) 暗号化コンテンツおよび購入受付データ送信

ショップサーバ100において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定すると、ショップサーバ100は、暗号化コンテンツおよび購入受付データをユーザ機器に送信する。これらは、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ：Kc (content) と、購入要求を受け付けたことを示すのみのデータであり、先のコンテンツキー：Kcをユーザ機器認証サーバ(DAS)300の公開鍵で暗号化した暗号化コンテンツ鍵データ：KpDAS(Kc)を含まないデータである。

【0184】購入受付データの構成を図32(h)に示す。購入受付データは、コンテンツ購入の要求元であるユーザ機器200の識別子であるユーザ機器ID、購入要求データ(図32(g)のユーザ機器公開鍵証明書を除いたデータ)、コンテンツ取り引きに伴いショップサーバ100が生成したショップ処理No.を有し、これらのデータに対するショップサーバ100の電子署名が付加されている。さらに、購入受付データには、ショップサーバ100の公開鍵証明書が添付され、ユーザ機器200に送付される。なお、ショップサーバ公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ユーザ機器側に送付済みの場合は、必ずしも改めて送付する必要はない。

【0185】(6) 受信データ検証

ショップサーバ100から暗号化コンテンツ：Kc (content) と、図32(h)に示す購入受付データを受信したユーザ機器200は、購入受付データの検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器200は、まずショップサーバ100から受領したショップサーバの公開鍵証明書の検証を発行局(CA)の公開鍵KpCAを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵KpSHOPを用いて図32(h)に示す購入受付データのショップ署名の検証を実行する。

【0186】(7) 相互認証

(8) 暗号化コンテンツ鍵データ1(ショップ)送信次にショップサーバ100は、ユーザ機器認証サーバ300にアクセスし、ショップサーバ100と、ユーザ機器認証サーバ300間において相互認証処理を実行する。相互認証が成立すると、ショップサーバ100は、ユーザ機器認証サーバ300に対して、暗号化コンテンツ鍵データ1(ショップ)を送信する。

【0187】暗号化コンテンツ鍵データ1(ショップ)の構成を図32(i)に示す。暗号化コンテンツ鍵データ1(ショップ)は、暗号化コンテンツ鍵かけかえ要求

の要求先であるユーザ機器認証サーバ300の識別子であるユーザ機器認証サーバID、ユーザ機器200から受領した購入要求データ(図32(g)のユーザ機器公開鍵証明書を除いたデータ)、ショップ処理No.を有し、これらのデータに対するショップサーバ100の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ1(ショップ)には、ショップサーバ100の公開鍵証明書と、ユーザ機器200の公開鍵証明書が添付され、ユーザ機器認証サーバ300に送付される。なお、ユーザ機器認証サーバ300がユーザ機器公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【0188】(9)受信データ検証

ショップサーバ100から暗号化コンテンツ鍵データ1(ショップ)(図32(i))を受信したユーザ機器認証サーバ300は、受信データの検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器認証サーバ300は、まずショップサーバ100から受領したショップサーバの公開鍵証明書の検証を発行局(CA)の公開鍵KpCAを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵KpSHOPを用いて図32(i)に示す暗号化コンテンツ鍵データ1(ショップ)の電子署名の検証を実行する。さらに、ユーザ機器の公開鍵証明書の検証を発行局(CA)の公開鍵KpCAを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵KpDEVを用いて図32(i)に示す暗号化コンテンツ鍵データ1(ショップ)に含まれる(3)購入要求データのユーザ機器署名の検証を実行する。

【0189】(10)暗号化コンテンツ鍵かけかえ処理
ユーザ機器認証サーバ300において、ショップサーバ100から受信した暗号化コンテンツ鍵データ1(ショップ)の検証が終了し、正当なデータであると判定すると、ユーザ機器認証サーバ300は、暗号化コンテンツ鍵データ1(ショップ)に含まれる暗号化コンテンツ鍵、すなわち、コンテンツ鍵:Kcをユーザ機器認証サーバ(DAS)300の公開鍵KpDASで暗号化したデータ:KpDAS(Kc)をユーザ機器認証サーバ300の秘密鍵KsDASで復号してコンテンツ鍵Kcを取得し、さらにコンテンツ鍵Kcをユーザ機器の公開鍵:KpDEVで暗号化した暗号化コンテンツ鍵:KpDEV(Kc)を生成する。すなわち、KpDAS(Kc)→Kc→KpDEV(Kc)の鍵かけかえ処理を実行する。この処理は、先に説明した図16に示すフローに従った処理である。

【0190】(11)暗号化コンテンツデータ送信

次に、ユーザ機器認証サーバ300は、暗号化コンテンツ鍵データ(DAS)をショップサーバ100に送信する。

【0191】暗号化コンテンツ鍵データ(DAS)の構

成を図33(j)に示す。暗号化コンテンツ鍵データ

(DAS)は、コンテンツ購入の要求先であるショップサーバ100の識別子であるショップID、暗号化コンテンツ鍵データ1(ショップ)(図32(i)のショップおよびユーザ機器公開鍵証明書を除いたデータ)、さらに、前述の鍵かけかえ処理により、ユーザ機器認証サーバ300が生成した暗号化コンテンツ鍵データ:KpDEV(Kc)を有し、これらのデータに対するユーザ機器認証サーバ300の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ(DAS)には、ユーザ機器認証サーバ300と、ユーザ機器200の公開鍵証明書が添付され、ショップサーバ100に送付される。なお、ショップサーバが、これらの公開鍵証明書を既に保有済みである場合は、必ずしも改めて送付する必要はない。

【0192】また、ユーザ機器認証サーバ300が信頼できる第三者機関であると認められる存在である場合は、暗号化コンテンツ鍵データ(DAS)は、図33(j)に示すような(8)暗号化コンテンツ鍵データ1(ショップ)をそのまま含むデータ構成とすることなく、図34(j')に示すように、ショップID、ユーザ機器ID、トランザクションID、コンテンツID、ショップ処理NO、ユーザデバイスの公開鍵で暗号化したコンテンツ鍵KpDEV(Kc)の各データを、ユーザ機器認証サーバ300が抽出して、これらに署名を付加して暗号化コンテンツ鍵データ(DAS)としてもよい。添付する公開鍵証明書は、ユーザ機器認証サーバ300の公開鍵証明書である。

【0193】(12)受信データ検証

ユーザ機器認証サーバ300から暗号化コンテンツ鍵データ(DAS)(図33(j))を受信したショップサーバ100は、暗号化コンテンツ鍵データ(DAS)の検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ショップサーバ100は、まずユーザ機器認証サーバ300から受領したユーザ機器認証サーバの公開鍵証明書の検証を発行局(CA)の公開鍵KpCAを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ300の公開鍵KpDASを用いて図33(j)に示す暗号化コンテンツ鍵データ(DAS)の電子署名の検証を実行する。なお、先に説明した図34(j')の簡略化した暗号化コンテンツ鍵データ(DAS)をショップサーバ100が受領した場合も同様の検証を実行する。さらに、必要に応じて図33(j)の暗号化コンテンツデータ(DAS)内の暗号化コンテンツ鍵1(ショップ1)を検証するようにしてもよい。

【0194】(13)相互認証、および

(14)暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器200は、暗号化コンテンツ鍵要求データをショップサーバに対して送信する。なお、この

際、前の要求と異なるセッションで要求を実行する場合は、再度相互認証を実行して、相互認証が成立したことを条件として暗号化コンテンツ鍵要求データがユーザ機器200からショップサーバ100に送信される。

【0195】(15) 検証処理、および

(16) 課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ100は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、図15を用いて説明したと同様の処理である。データ検証が済むと、ショップサーバ100は、コンテンツの取り引きに関する課金処理を実行する。課金処理は、ユーザの取り引き口座からコンテンツ料金を受領する処理である。受領したコンテンツ料金は、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に配分される。

【0196】前述した基本モデル1と同様、この課金処理に至るまでには、ユーザ機器認証サーバ300による暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となっているので、ショップサーバ100は、ユーザ機器間とのみの処理では課金処理が実行できない。また、ユーザ機器200においても暗号化コンテンツ鍵の復号ができないので、コンテンツの利用ができない。ユーザ機器認証サーバは、図6を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべての課金対象となるコンテンツ取り引きが把握可能となる。従って、ショップ側単独でのコンテンツ取り引きは不可能となり、不正なコンテンツ販売が防止される。

【0197】(17) 暗号化コンテンツ鍵データ2 (ショップ) 送信

ショップサーバ100における課金処理が終了すると、ショップサーバ100は、暗号化コンテンツ鍵データ2 (ショップ) をユーザ機器200に送信する。

【0198】暗号化コンテンツ鍵データ2 (ショップ) の構成を図33 (k) に示す。暗号化コンテンツ鍵データ2 (ショップ) は、暗号化コンテンツ鍵要求の要求元であるユーザ機器200の識別子であるユーザ機器ID、ユーザ機器認証サーバ300から受領した暗号化コンテンツ鍵データ (DAS) (図33 (j) のユーザ機器認証サーバ公開鍵証明書を除いたデータ)、を有し、これらのデータに対するショップサーバ100の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ2 (ショップ) には、ショップサーバ100の公開鍵証明書と、ユーザ機器認証サーバ300の公開鍵証明書が添付され、ユーザ機器200に送付される。なお、ユーザ機器200がユーザ機器認証サーバ公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【0199】なお、ユーザ機器認証サーバ300が信頼できる第三者機関であると認められる存在であり、ショップサーバ100がユーザ機器認証サーバ300から受信する暗号化コンテンツ鍵データ (DAS) が先に説明した図34 (j') の簡略化した暗号化コンテンツ鍵データ (DAS) である場合は、ショップサーバ100は、図34 (k') に示す暗号化コンテンツ鍵データ2 (ショップ) をユーザ機器に送付する。すなわち、図34 (j') に示す簡略化した暗号化コンテンツ鍵データ (DAS) にショップサーバの署名を付加したデータに、ショップサーバ100の公開鍵証明書と、ユーザ機器認証サーバ300の公開鍵証明書を添付してユーザ機器200に送付する。

【0200】(18) 受信データ検証

ショップサーバ100から、暗号化コンテンツ鍵データ2 (ショップ) を受領したユーザ機器200は、暗号化コンテンツ鍵データ2 (ショップ) の検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器200は、まずショップサーバ100から受領したショップサーバの公開鍵証明書の検証を発行局 (CA) の公開鍵 K_{pCA} を用いて実行し、次に公開鍵証明書から取り出したショップサーバ100の公開鍵 K_{pSHOP} を用いて図33 (k) に示す暗号化コンテンツ鍵データ2 (ショップ) の電子署名の検証を実行する。さらに、ユーザ機器認証サーバ300の公開鍵証明書の検証を発行局 (CA) の公開鍵 K_{pCA} を用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ300の公開鍵 K_{pDAS} を用いて図33 (j) に示す暗号化コンテンツ鍵データ2 (ショップ) に含まれる (11) 暗号化コンテンツ鍵データ (DAS) の署名検証を実行する。さらに、必要に応じて図33 (j) の暗号化コンテンツデータ (DAS) 内の暗号化コンテンツ鍵1 (ショップ1) を検証するようにしてもよい。

【0201】(19) 保存処理

ショップサーバ100から受信した暗号化コンテンツ鍵データ2 (ショップ) を検証したユーザ機器200は、暗号化コンテンツ鍵データ2 (ショップ) に含まれる自己の公開鍵 K_{pDEV} で暗号化された暗号化コンテンツ鍵: $K_{pDEV} (K_c)$ を自己の秘密鍵 K_{sDEV} を用いて復号し、さらに、ユーザ機器の保存鍵 K_{sto} を用いて暗号化して暗号化コンテンツ鍵: $K_{sto} (K_c)$ を生成して、これをユーザ機器200の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵: $K_{sto} (K_c)$ を保存鍵 K_{sto} を用いて復号してコンテンツ鍵 K_c を取り出して、取り出したコンテンツ鍵 K_c を用いて、暗号化コンテンツ K_c (Content) の復号処理を実行し、コンテンツ (Content) を再生、実行する。

【0202】このように、基本配信モデル2において

は、ユーザ機器200と、ユーザ機器認証サーバ300との間ではデータの送受信が実行されず、ユーザ機器200は、ショップサーバ100との間でデータ送受信を行なうのみでよく、ユーザ機器の処理負担が軽減される。

【0203】[1. 2. 基本コンテンツ配信モデル2の変形例] 次に、図31に示した基本コンテンツ配信モデル2の構成の変形例について説明する。図35に示す構成は、ショップサーバの機能を分離し、ショップサーバと配信サーバを設けた構成である。ショップサーバ100は、ユーザ機器200からのコンテンツ購入要求を受領するが、ユーザ機器200に対するコンテンツ配信は配信サーバ400が実行する。本構成では、データ送受信を実行するエンティティ間での相互認証を行わず、各エンティティは、受信データの署名検証のみを行なう。しかし、基本コンテンツ配信モデル2同様、エンティティ間で相互認証処理を行なう構成をとっても構わない。

【0204】ショップサーバ100は、ユーザ機器200からの購入要求データを受信し、データの検証(図35の処理(3))を行なって、要求データの正当性を確認した後、配信サーバ400に対して、コンテンツ配信要求の送信を実行(図35の処理(4))する。配信サーバ400は、ショップサーバ100からのコンテンツ配信要求データを検証し、データの正当性が確認された場合、コンテンツデータベース410から取り出した暗号化コンテンツを送信(図35の処理(6))する。

【0205】ユーザ機器200は、配信サーバ400から、暗号化コンテンツを受信し、データ検証の後、暗号化コンテンツ受領データを配信サーバ400に送信(図35の処理(8))する。配信サーバ400は、受信データ検証の後、ユーザ機器認証サーバ300に対して暗号化コンテンツ鍵データ(配信サーバ)および暗号化コンテンツ鍵かけかえ要求を送信(図35の処理(10))する。

【0206】ユーザ機器認証サーバ300が配信サーバ400から暗号化コンテンツ鍵データ(配信サーバ)および暗号化コンテンツ鍵かけかえ要求を受信した以後の処理は、相互認証処理を省略した以外は、先の図31に示した構成に基づく実施例と同様となる。

【0207】本構成においては、ユーザ機器は、相互認証を行わずに、ショップサーバに対してコンテンツ購入要求を送信し、配信サーバから暗号化コンテンツを受領する。ショップサーバ100は、ユーザ機器からのコンテンツ要求を受け付けて、その正当性を署名検証のみに基づいて検証する。さらに、ユーザ機器認証サーバからの、かけかえ済みの暗号化コンテンツ鍵を受信し、その正当性を署名検証により実行する。配信サーバ400は、ショップサーバからの受信データについての署名検証を実行してデータ正当性の確認を行ないコンテンツ配

信を行なう。

【0208】ショップサーバ100は、コンテンツ自体の管理、配信を行なわない。従って、例えば音楽データを管理する音楽コンテンツ配信サーバ、ゲームコンテンツを管理するゲームコンテンツ配信サーバ等、様々なコンテンツ管理主体となる複数の配信サーバに対して1つのショップサーバがユーザ機器からのコンテンツ要求に応答し、ショップサーバが要求に応じて要求コンテンツを管理する配信サーバにコンテンツ配信要求を送信する構成に適した態様である。また、この構成にしたことにより、例えば、ユーザ機器とショップサーバは双方向通信であるため、インターネットを使うが、配信サーバからユーザ機器へは片方向通信であるため、高速な衛星通信が利用できるメリットがある。

【0209】本実施例では、相互認証が省略され、署名検証のみにより、データの正当性を確認する処理としたので、処理の効率化が実現される。

【0210】図36は、図35と同様ショップサーバの機能を分離し、ショップサーバと配信サーバを設け、相互認証を省略した構成であり、ショップサーバ100は、ユーザ機器200からのコンテンツ購入要求を受領し、署名検証を行なう。ユーザ機器200に対するコンテンツ配信は配信サーバ400が実行する。図35の構成と異なる点は、ショップサーバ100から配信サーバ400に対してコンテンツ配信要求を送信せず、ユーザ機器認証サーバ300が、配信サーバ400に対してコンテンツ配信要求を送信する構成とした点である。

【0211】ショップサーバ100は、ユーザ機器200からの購入要求データを受信し、データの検証(図36の処理(3))を行なって、要求データの正当性を確認した後、ユーザ機器認証サーバ300に対して、暗号化コンテンツ鍵データ1(ショップ)の送信を実行(図36の処理(4))する。その後、ユーザ機器認証サーバ300は、データの検証(図36の処理(5))を行なって、要求データの正当性を確認した後、配信サーバ400に対して、コンテンツ配信要求の送信を実行(図36の処理(6))する。配信サーバ400は、ユーザ機器認証サーバ300からのコンテンツ配信要求データを検証し、正当性が確認された場合、ユーザ機器200に対して、コンテンツデータベース410から取り出した暗号化コンテンツを送信(図36の処理(8))する。以後の処理は、先の図35に示した構成に基づく処理と同様となる。

【0212】本構成においては、ユーザ機器認証サーバ300は、配信サーバ400からの鍵のかけかえ要求以前、ショップサーバ100に対してコンテンツ購入要求があった時点で、コンテンツ購入要求主体であるユーザ機器情報を取得し、管理することが可能となる。従って、配信サーバ400からの鍵のかけかえ要求受領時に、すでに登録済みのコンテンツ購入要求ユーザ機器で

あるか否かの照合処理が可能となる。また、DASが信頼できる機関であるとみなせば、配信サーバはショップサーバの送信データを検証しなくてもよくなり、処理の効率化が図れる。

【0213】以上、説明したように、本発明のコンテンツ配信構成によれば、ユーザ機器は、暗号化コンテンツKc (Content) 取得後、コンテンツ利用可能な状態に至るまでには、ユーザ機器認証サーバにおける暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となる。従って、ショップサーバが、ユーザ機器に対して、ユーザ機器認証サーバに通知せずコンテンツを販売し、コンテンツをユーザ機器において利用可能な状態とすることができない。ユーザ機器認証サーバは、ユーザ機器認証サーバ・ライセンス管理データベース (図6参照) に、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべてのショップの取り引きの管理が可能であり、課金されたコンテンツ取り引きを把握し、ショップの課金処理において受領されたコンテンツ料金を、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に正確に配分することが可能となり、不正なコンテンツ利用を排除する構成が実現される。

【0214】[2. 電子チケットを利用したコンテンツ配信モデル] 次に、ユーザによるコンテンツの利用 (購入) に基づいて、コンテンツの著作権者、製作者、ライセンスホルダー、ショップ等、様々な関係者に対する利益配分情報を記述した電子チケットを発行して、発行した電子チケットに基づく利益配分処理を実行する構成について説明する。

【0215】図37に電子チケットに基づく利益配分を実行するシステム構成を示す。図37のコンテンツ配信システムは、ユーザ機器が購入するコンテンツの購入要求を受け付け、コンテンツ購入に伴う利用料金の利益配分情報を記述した電子チケットを発行するチケット発行サーバ (TIS: Ticket Issuer Server) 610、コンテンツ購入主体となるユーザ機器 (DEV) 620、正当なコンテンツ取り引き管理のための鍵かけかえ処理を行なう管理サーバとして機能するユーザ機器認証サーバ (DAS: Device Authentication Server) 630、コンテンツの配信を行なうコンテンツプロバイダ (CP) 等の配信サーバ (CP: Content Provider) 640、さらに、電子チケットに基づいて利用料金の振替等の換金処理を行なうチケット換金サーバ (TES: Ticket Exchange Server) 650を主構成要素とする。

【0216】(チケット発行サーバ) 図37のコンテンツ配信システムのチケット発行サーバ (TIS) 610の構成を図38に示す。チケット発行サーバ610は、ユーザ機器620からの購入要求を受け付け、購入要求のあった取り引き対象となるコンテンツに対応してその利益配分情報を記述した電子チケットを発行する。

【0217】チケット発行サーバ (TIS) 610は、コンテンツ取り引きに伴う発行チケットの管理データ、例えばコンテンツ販売先のユーザ機器の識別子とコンテンツ識別子、コンテンツ料金等を対応づけて管理するチケット発行管理データベース612を有する。さらに、ユーザ機器620からのコンテンツ購入要求検証、チケット発行管理データベースの制御、チケットに基づくユーザ機器に対する課金処理、ユーザ機器等との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段613を有する。

【0218】チケット発行管理データベース612のデータ構成を図39に示す。チケット発行管理データベース612は、チケット発行サーバがコンテンツ取り引きに応じてチケット発行処理を実行する際に内部生成する識別番号としてのチケット発行処理No.、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ID、ユーザ機器とチケット発行サーバ間での取り引きを実行する際に、コンテンツ取り引き識別子としてユーザ機器で生成発行するトランザクションID、取り引き対象コンテンツの識別子であるコンテンツID、チケット発行サーバ610の発行する電子チケットに基づいて対価を得るエンティティ、例えば著作権者、ライセンスホルダ、管理者、コンテンツ販売関係者等の識別子としてのチケット利用先ID、各チケット利用先IDに対応するコンテンツ利用料金配分金額としての金額、チケットに基づく換金処理の有効期限、チケット発行サーバ610におけるチケット発行、管理処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【0219】チケット発行サーバ610の制御手段613は、図38に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段613は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段613の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。チケット発行サーバ610が格納する暗号鍵等の暗号処理用データとしては、チケット発行サーバ610の秘密鍵: KsTIS、チケット発行サーバ610の公開鍵証明書Cert_TIS、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局 (CA: Certificate Authority) の公開鍵KpCAがある。

【0220】制御手段613の構成は、先に図4を用いて説明した制御手段構成と同様の構成、すなわち、中央演算処理装置 (CPU: Central Processing Unit)、ROM (Read only Memory)、RAM (Random Access Memory)、表示部、入力部、記憶手段、通信インタフェース等を持つ構成である。

【0221】(ユーザ機器) ユーザ機器 (DEV) 62

0は、図1の構成におけるユーザ機器、すなわち、図7の構成と同様の構成を持つ。ユーザ機器620が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器の秘密鍵：KsDEV、ユーザ機器の公開鍵証明書Cert_DEV、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（CA：Certificate Authority）の公開鍵KpCA、コンテンツをユーザ機器の例えばハードディスク等の記憶手段に格納する際の暗号化鍵として適用する保存鍵Kstoがある。

【0222】図37のチケット管理構成を実行するシステムにおけるユーザ機器620の有する購入管理データベースは、チケット管理機能を持つデータ構成となる。購入管理データベースのデータ構成を図40に示す。購入管理データベースは、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するトランザクションID、取り引き対象コンテンツの識別子であるコンテンツID、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ID、チケット発行サーバ610が設定するチケット発行処理No.、チケットを送信した先の送信先エンティティの識別子としてのチケット送信先ID、さらに、ユーザ機器におけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【0223】（ユーザ機器認証サーバ）ユーザ機器認証サーバ（DAS）630は、図1の構成におけるユーザ機器認証サーバ、すなわち、図5の構成と同様の構成を持つ。ユーザ機器認証サーバ630が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器認証サーバ（DAS）の秘密鍵：KsDAS、ユーザ機器認証サーバ（DAS）の公開鍵証明書Cert_DAS、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（CA：Certificate Authority）の公開鍵KpCAがある。

【0224】図37のチケット管理構成を実行するシステムにおけるユーザ機器認証サーバ630の有するライセンス管理データベースは、チケット管理機能を持つデータ構成となる。ライセンス管理データベースのデータ構成を図41に示す。ライセンス管理データベースは、コンテンツ取り引き時にユーザ機器認証サーバ（DAS）630の実行する処理に応じて内部生成する処理識別子としてのユーザ機器認証サーバ処理No.、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ID、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するトランザクションID、取り引き対象コンテンツの識別子であるコンテンツID、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ID、チケット発行サーバ610が設定するチケット発行処理No.、さらに、ユーザ

機器認証サーバ（DAS）におけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【0225】（配信サーバ）図37のコンテンツ配信システムの配信サーバ640の構成を図42に示す。配信サーバ640は、例えばコンテンツプロバイダ（CP）であり、取り引き対象となるコンテンツをコンテンツキーで暗号化した暗号化コンテンツデータであるKc（Content）と、コンテンツキーKcをユーザ機器認証サーバ（DAS：Device Authentication Server）の公開鍵：KpDASで暗号化した暗号化コンテンツキーKpDAS（Kc）を格納したコンテンツデータベース644を有する。なお、暗号化コンテンツデータであるKc（Content）は、図にも示すように、それぞれコンテンツ識別子であるコンテンツIDが付加され、コンテンツIDに基づいて識別可能な構成を持つ。

【0226】配信サーバ640は、さらにコンテンツの配信管理データを管理する配信管理データベース642を有する。配信管理データベース642は、チケット管理機能を持つデータ構成となる。購入管理データベースのデータ構成を図43に示す。配信管理データベース642は、コンテンツ配信処理を実行する際に、配信サーバ640が設定する配信サーバ処理No.、取り引き対象コンテンツの識別子であるコンテンツID、コンテンツの配信対象識別子としてのユーザ機器ID、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ID、チケット発行体が設定するチケット発行処理No.、さらに、配信サーバにおけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【0227】さらに、配信サーバ640は、コンテンツデータベース644からの配信コンテンツの抽出処理、取り引きに伴う配信管理データベース642に対して登録する取り引きデータの生成処理、ユーザ機器620他との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段643を有する。制御手段643は、図42に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段643は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段643の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。配信サーバ640が格納する暗号鍵等の暗号処理用データとしては、配信サーバ640の秘密鍵：KsCP、配信サーバ640の公開鍵証明書Cert_CP、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（CA：Certificate Authority）

y) の公開鍵 K_{pCA} がある。

【0228】制御手段643の構成は、先に図4を用いて説明した制御手段構成と同様の構成、すなわち、中央演算処理装置 (CPU: Central Processing Unit)、ROM (Read only Memory)、RAM (Random Access Memory)、表示部、入力部、記憶手段、通信インタフェース等を持つ構成である。

【0229】(チケット換金サーバ) 図37のコンテンツ配信システムのチケット換金サーバ (TES) 650の構成を図44に示す。チケット換金サーバ650は、様々なエンティティから電子チケットを受信し、受信データの検証の後、チケットに基づく換金処理、例えば口座振替処理、あるいは電子マネーの残高変更処理等を行なう、具体的な一例としては、チケット換金サーバ650は各エンティティの銀行口座を管理する銀行内のサーバとする設定が可能である。

【0230】チケット換金サーバ650は、コンテンツ取り引きに伴う発行チケットに基づく換金処理の管理データを管理するチケット換金管理データベース652を有する。さらに、各エンティティからの受信チケット検証、チケット換金管理データベースの制御、各エンティティとの通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段653を有する。

【0231】チケット換金管理データベース652のデータ構成を図45に示す。チケット換金管理データベース652は、チケット換金サーバが受領チケットに応じてチケット換金処理を実行する際に内部生成する識別番号としてのチケット換金サーバ処理No.、チケットに基づく換金の要求を行なってきた要求主体識別子としての換金依頼元ID、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ID、チケット発行サーバ610が設定するチケット発行処理No.、チケットに基づく換金金額、コンテンツの購入主体であるユーザ機器の識別子としてのユーザ機器ID、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するトランザクションID、さらに、チケット換金サーバにおける換金処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【0232】さらに、チケット換金サーバ650は、チケット換金管理データベース652のデータ生成、更新処理、受領チケットの検証処理、各種エンティティとの通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段653を有する。制御手段653は、図44に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段653は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段653の暗号処理手段において実行される暗号処理において使用される鍵デ

ータ等は、制御手段内部の記憶手段にセキュアに格納されている。チケット換金サーバ650が格納する暗号鍵等の暗号処理用データとしては、チケット換金サーバ650の秘密鍵: K_{sTES} 、チケット換金サーバ650の公開鍵証明書 $Cert_{TES}$ 、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局 (CA: Certificate Authority) の公開鍵 K_{pCA} がある。

【0233】制御手段653の構成は、先に図4を用いて説明した制御手段構成と同様の構成、すなわち、中央演算処理装置 (CPU: Central Processing Unit)、ROM (Read only Memory)、RAM (Random Access Memory)、表示部、入力部、記憶手段、通信インタフェース等を持つ構成である。

【0234】[コンテンツ購入処理] 次に、図37に戻り、ユーザ機器が、チケット発行サーバにコンテンツ購入要求を発行してコンテンツを利用可能な状態としてユーザ機器に保存し、チケットに基づいてコンテンツ料金が配分 (換金) されるまでの処理について説明する。図37の番号 (1) から (32) の順に処理が進行する。各番号順に処理の詳細を説明する。

【0235】(1) 相互認証

コンテンツを購入しようとするユーザ機器620は、チケット発行サーバ610との間で相互認証処理を行なう。相互認証処理は、図12または図13を用いて説明した処理である。相互認証処理において、生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。

【0236】(2) トランザクションID、購入要求データ生成、および

(3) 購入要求データ送信

チケット発行サーバ610とユーザ機器620間の相互認証が成功すると、ユーザ機器620は、コンテンツの購入要求データを生成する。購入要求データの構成を図46 (m) に示す。購入要求データは、コンテンツ購入の要求元であるユーザ機器620の識別子である機器ID、取り引きの識別子として、ユーザ機器620の暗号処理手段が例えば乱数に基づいて生成するトランザクションID、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツIDの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、購入要求データには、署名検証に必要に応じてユーザ機器の公開鍵証明書を添付する。

【0237】(4) 受信データ検証

図46 (m) に示す購入要求データをユーザ機器620から受信したチケット発行サーバ610は、受信データの検証処理を実行する。検証処理の詳細は、先に図15を用いて説明した通りである。

【0238】(5) 課金処理

(6) 電子チケット発行

(7) 電子チケット送信

チケット発行サーバ610は、次に、コンテンツの取り引きに関する課金処理、電子チケット発行処理を実行する。これらの処理は、例えば予め登録されているユーザ口座、あるいは電子マネー口座等に基づいて設定されるユーザの取り引き金額限度内の電子チケットを発行する処理として実行される。発行された電子チケットは、ユーザ機器620に送信される。

【0239】電子チケットの構成例を図47に示す。図47(A)は、電子チケットに基づく料金配分先(料金受領エンティティ)が単一である場合のデータ構成であり、チケット発行体ID、チケット発行処理No.、電子チケットに基づく料金配分先(エンティティ)を示すチケット利用先ID、電子チケットに基づいて配分される料金を示す金額、電子チケットの有効期限、すなわち料金受領エンティティがチケットに基づく換金(料金精算)処理を実行可能な期限、さらに、ユーザ機器からチケット発行サーバに対して送信された購入要求データ

(図46(m)参照)を含む。なお、さらに、チケット発行日等のデータを付加してもよい。これらのデータにチケット発行サーバ610の電子署名が付加される。さらに、電子チケットには、署名検証用に必要に応じてチケット発行サーバの公開鍵証明書を添付する。

【0240】図47(B)は、電子チケットに基づく料金配分先(エンティティ)が複数である場合のデータ構成であり、チケット利用先IDが複数(1~n)格納され、それぞれのチケット利用先ID毎に、電子チケットに基づいて配分される料金を示す金額が1~nまで格納されている。チケットに基づいて料金を受領するエンティティは、自己のIDに対応する金額を受領する。

【0241】図37の処理例では、チケット発行サーバ610は、配信サーバを管理するコンテンツプロバイダ(CP)用の電子チケットと、ユーザ機器認証サーバ(DAS)用の電子チケットを発行する。これらのチケット発行先は、コンテンツ毎に異なり、コンテンツの著作権等が含まれる場合もある。チケット発行サーバは、コンテンツIDに基づいてチケット発行先と、配分金額を定めたテーブルを有し、ユーザ機器からのコンテンツ購入要求に含まれるコンテンツIDに基づいてテーブルからチケット発行先と、配分金額データを取得してチケットを生成して発行する。

【0242】(8) 受信データ検証

チケット発行サーバ610からチケットを受信したユーザ機器620は、チケットの検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器620は、まずチケット発行サーバの公開鍵証明書の検証を発行局(CA)の公開鍵KpCAを用いて実行し、次に公開鍵証明書から取り出したチケット発行サーバの公開鍵KpTISを用いてチケットの署名検証を実行する。

【0243】(9) 相互認証

(10) 電子チケット(CP用)送信

次にユーザ機器620は、配信サーバ640にアクセスし、相互認証処理を実行する。相互認証が成立すると、ユーザ機器620は、配信サーバ640に対して、配信サーバ用の電子チケット(CP用)を送信する。

【0244】(11) 受信データ検証

(12) 暗号化コンテンツおよび暗号化コンテンツ鍵送信

配信サーバ640において、電子チケット(CP用)の検証が完了し、データ改竄のない正当な電子チケットであると判定すると、配信サーバ640は、暗号化コンテンツおよび暗号化コンテンツ鍵をユーザ機器に送信する。これらは、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ:Kc(content)と、コンテンツキー:Kcをユーザ機器認証サーバ(DAS)630の公開鍵で暗号化した暗号化コンテンツ鍵データ:KpDAS(Kc)を含むデータである。

【0245】(13) 受信データ検証

(14) 相互認証

(15) 電子チケット(DAS用)および鍵かけかえ要求送信

配信サーバ640から暗号化コンテンツおよび暗号化コンテンツ鍵を受信したユーザ機器620は、データの検証処理を実行する。データ検証後、ユーザ機器620は、ユーザ機器認証サーバ630にアクセスし、相互認証処理を実行する。相互認証が成立すると、ユーザ機器620は、ユーザ機器認証サーバ630に対して、ユーザ機器認証サーバ用の電子チケット(DAS)および鍵かけかえ要求を送信する。鍵かけかえ要求は、先に配信サーバ640から受信したユーザ機器認証サーバの公開鍵で暗号化されたコンテンツ鍵Kcである。暗号化コンテンツ鍵KpDAS(Kc)をユーザ機器の公開鍵KpDEVで暗号化したコンテンツ鍵、すなわちKpDEV(Kc)とする処理を要求するものであり、図1を用いて説明したかけかえ処理と同様である。

【0246】(16) 受信データ検証

(17) 暗号化コンテンツ鍵かけかえ処理、

ユーザ機器620から電子チケット(DAS用)および暗号化コンテンツ鍵KpDAS(Kc)のかけかえ要求を受信したユーザ機器認証サーバ630は、電子チケット(DAS用)、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。検証が終了し、データの改竄のない正当な電子チケットであり、正当な鍵かけかえ要求であると判定すると、ユーザ機器認証サーバ630は、コンテンツ鍵:Kcをユーザ機器認証サーバ(DAS)630の公開鍵KpDASで暗号化したデータ:KpDAS

(Kc)をユーザ機器認証サーバ630の秘密鍵KsDASで復号してコンテンツ鍵Kcを取得し、さらにコンテンツ鍵Kcをユーザ機器の公開鍵:KpDEVで暗号

化した暗号化コンテンツ鍵: K_pDEV (K_c) を生成する。すなわち、K_pDAS (K_c) → K_c → K_pDEV (K_c) の鍵かけかえ処理を実行する。この処理は、前述の図16を用いて説明した処理と同様である。

【0247】 (18) 暗号化コンテンツ鍵送信

(19) 受信データ検証

(20) 保存処理

ユーザ機器認証サーバ630は、鍵かけかえにより生成した暗号化コンテンツ鍵K_pDEV (K_c) をユーザ機器620に送信する。ユーザ機器認証サーバ630から、暗号化コンテンツ鍵K_pDEV (K_c) を受領したユーザ機器620は、受信データ検証処理を実行し、検証後、ユーザ機器620は、暗号化コンテンツ鍵K_pDEV (K_c) を自己の秘密鍵K_sDEVを用いて復号し、さらに、ユーザ機器の保存鍵K_{sto}を用いて暗号化して暗号化コンテンツ鍵: K_{sto} (K_c) を生成して、これをユーザ機器620の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵: K_{sto} (K_c) を保存鍵K_{sto}を用いて復号してコンテンツ鍵K_cを取り出して、取り出したコンテンツ鍵K_cを用いて、暗号化コンテンツK_c (Content) の復号処理を実行し、コンテンツ (Content) を再生、実行する。

【0248】 (21) 相互認証

(22) 電子チケット (CP用) 送信

配信サーバ640は、ユーザ機器620に対する暗号化コンテンツ配信の後、チケット換金サーバ650にアクセスし、相互認証処理を実行する。相互認証が成立すると、配信サーバ640は、チケット換金サーバ650に対して、配信サーバ用の電子チケット (CP用) を送信する。

【0249】 (23) 受信データ検証、換金処理

チケット換金サーバ650において、電子チケット (CP用) の検証が完了し、データ改竄のない正当な電子チケットであると判定すると、チケット換金サーバ650は、受領した電子チケット (CP用) に基づいて換金処理を実行する。換金処理は、例えば予め登録されている配信サーバを管理するコンテンツプロバイダ (CP) の管理口座、あるいは電子マネー口座等に、電子チケット (CP用) に設定された金額をユーザ機器の管理ユーザの口座から振り替える処理として行われる。あるいは既にチケット発行サーバがユーザからの前払い預り金として受領しているチケット発行サーバ管理口座からコンテンツプロバイダ (CP) の管理口座にチケットに設定された金額を振り替える処理として行なってもよい。なお、チケット換金サーバ650は、チケットに格納された有効期限を検証し、有効期限内であることが確認されたことを条件として該チケットに基づく料金精算処理を実行する。

【0250】 (24) 換金処理レポート報告

チケット換金サーバ650において、電子チケット (C

P用) に基づく換金が終了すると、チケット換金サーバ650は、配信サーバ640に対して換金処理が済んだことを示すレポートを送信する。

【0251】 換金処理レポートの構成例を図46 (n) に示す。換金処理レポートは、チケット換金処理個々の識別子であるチケット換金処理ID、チケットに基づく換金の要求を行なってきた要求主体識別子としての換金依頼元ID、チケットに基づく換金金額、コンテンツ取り引きに伴いチケットを発行したチケット発行体の識別子であるチケット発行体ID、チケット発行サーバ610が設定するチケット発行処理No.、チケット換金サーバ650において換金処理が実行されたチケット換金処理完了日等のデータを有し、これらにチケット換金サーバ650の電子署名が付加される。さらに、換金処理レポートには、署名検証用に必要に応じてチケット換金サーバの公開鍵証明書を添付する。

【0252】 (25) 受信データ検証

チケット換金サーバ650から換金処理レポートを受信した配信サーバ640は、換金処理レポートの検証処理を実行する。データ検証により、レポートが正当であると認められれば、配信サーバの管理主体であるコンテンツプロバイダに対するコンテンツ取り引きに伴う料金配分が完了したことが確認される。

【0253】 (26) 相互認証

(27) 電子チケット (DAS用) 送信

(28) 受信データ検証、換金処理

(29) 換金処理レポート報告

(30) 受信データ検証

ユーザ機器認証サーバ630とチケット換金サーバ650との間においても、上述の配信サーバ640とチケット換金サーバ650間の処理 (21) ~ (25) と同様の処理が電子チケット (DAS用) に基づいて実行される。

【0254】 (31) 相互認証

(32) 換金処理レポート報告

(33) 受信データ検証

また、チケット換金サーバ650は、各エンティティから受領したチケットに基づいて換金処理を実行した場合、チケット発行サーバ610との相互認証後、各エンティティに送付したと同様の換金処理レポート (図46 (n) 参照) をチケット発行サーバ610に送信する。チケット発行サーバ610は、チケット換金サーバ650から受信した換金処理レポートの検証を実行し、発行したチケットに関する換金処理が完了したことを確認する。

【0255】 (各機器におけるステータス遷移) 図37に示すチケット発行サーバ610等の各エンティティは、それぞれコンテンツ取り引きに係る一連の処理において、処理状態を示すステータスに応じて、次の処理を決定する。ステータスは、例えば図39に示すチケット

発行管理データベース、図40のユーザ機器の購入管理データベース等において、各コンテンツ取り引き毎に管理される。

【0256】まず、チケット発行サーバ610のステータス遷移について、図48を用いて説明する。チケット発行サーバ610は、ユーザ機器620からのコンテンツ購入要求データを受信(図37の処理(3)に対応)することで処理が開始される。チケット発行サーバ610は、ユーザ機器620からの受信データを検証し、検証に成功した場合は、ステータスを「購入受付完了」に設定し、データ検証により正当な購入要求であるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、購入受付処理を所定回数繰り返した後処理を中止し、ステータスを「購入受付失敗」とする。ステータスが「購入受付完了」である場合にのみ次ステップに進む。

【0257】ステータスが「購入受付完了」に遷移すると、次に、チケット発行サーバ610は、ユーザ機器620に対して電子チケットを送信(図37の処理(7)に対応)し、ユーザ機器からの受信応答(レスポンス)を受領することにより、ステータスを「チケット配信完了」とする。受信応答(レスポンス)を受領しなかった場合は、処理を中止するか、あるいは同様の処理、ここでは、電子チケットの送信処理を所定回数繰り返した後、処理を中止し、ステータスを「チケット配信失敗」とする。ステータスが「チケット配信完了」である場合にのみ次ステップに進む。

【0258】ステータスが「チケット配信完了」に遷移した場合、次に、チケット発行サーバ610は、チケット換金サーバから換金処理レポートを受信し、レポートの検証(図37の処理(32)、(33)に対応)を実行する。検証に成功した場合は、ステータスを「換金処理レポート受信完了」に設定し、処理終了とする。レポート検証により正当なレポートであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、レポート受信、検証処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート受信失敗」とする。チケット発行サーバ610は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【0259】次にユーザ機器認証サーバ630のステータス遷移について、図49を用いて説明する。ユーザ機器認証サーバ630は、ユーザ機器620からの暗号化コンテンツ鍵KpDAS(Kc)を受信(図37の処理(15)に対応)することで処理が開始される。ユーザ機器認証サーバ630は、ユーザ機器620からの電子チケット(DAS)を含む受信データを検証し、検証に成功した場合は、ステータスを「鍵受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは

同様の処理、ここでは、暗号化コンテンツ鍵データ(ユーザ機器)の受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵受信失敗」とする。ステータスが「鍵受信完了」である場合にのみ次ステップに進む。

【0260】ステータスが「鍵受信完了」に遷移すると、次に、ユーザ機器認証サーバ630は、コンテンツ鍵かけかえ処理(図37の処理(17)に対応)を実行し、鍵かけかえ処理が成功した場合には、ステータスを「鍵かけかえ完了」とする。鍵かけかえに失敗することは想定していないので、ここでは「鍵かけかえ完了」のみのステータス遷移が存在する。

【0261】ステータスが「鍵かけかえ完了」に遷移した場合、次に、ユーザ機器認証サーバ630は、ユーザ機器620に対して暗号化コンテンツ鍵データ(DAS)を送信(図37の処理(18)に対応)し、ユーザ機器620からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「鍵送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ(DAS)の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵送信失敗」とする。

【0262】ステータスが「鍵送信完了」に遷移すると、次に、ユーザ機器認証サーバ630は、チケット換金サーバ650に対して、電子チケット(DAS用)を送信(図37の処理(27)に対応)し、チケット換金サーバ650からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「チケット換金要求送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケット換金要求の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「チケット換金要求失敗」とする。

【0263】ステータスが「チケット換金要求送信完了」に遷移すると、次に、ユーザ機器認証サーバ630は、チケット換金サーバ650からの換金処理レポートを受信し、レポートの検証処理(図37の処理(29)、(30)に対応)を実行する。検証に成功した場合は、ステータスを「換金処理レポート受信完了」に設定し、処理終了とする。レポート検証により正当なレポートであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、レポート受信、検証処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート受信失敗」とする。ユーザ機器認証サーバ630は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【0264】次に配信サーバ640のステータス遷移について、図50を用いて説明する。配信サーバ640は、ユーザ機器620からの電子チケット(CP用)を

受信（図37の処理（10）に対応）することで処理が開始される。配信サーバ640は、ユーザ機器620からの受信データを検証し、検証に成功した場合は、ステータスを「電子チケット受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケットの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット受信失敗」とする。ステータスが「電子チケット受信完了」である場合にのみ次ステップに進む。

【0265】ステータスが「電子チケット受信完了」に遷移すると、次に、配信サーバ640は、ユーザ機器620に対して暗号化コンテンツおよび暗号化コンテンツ鍵データKpDAS（Kc）を送信（図37の処理（12）に対応）し、ユーザ機器620からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「配信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツおよび暗号化コンテンツ鍵データKpDAS（Kc）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「配信失敗」とする。

【0266】ステータスが「配信完了」に遷移すると、次に、配信サーバ640は、チケット換金サーバ650に対して、電子チケット（CP用）を送信（図37の処理（22）に対応）し、チケット換金サーバ650からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「チケット換金要求送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケット換金要求の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「チケット換金要求失敗」とする。

【0267】ステータスが「チケット換金要求送信完了」に遷移すると、次に、配信サーバ640は、チケット換金サーバ650からの換金処理レポートを受信し、レポートの検証処理（図37の処理（24）、（25）に対応）を実行する。検証に成功した場合は、ステータスを「換金処理レポート受信完了」に設定し、処理終了とする。レポート検証により正当なレポートであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、レポート受信、検証処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート受信失敗」とする。配信サーバ640は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【0268】次に、ユーザ機器620のステータス遷移について、図51を用いて説明する。ユーザ機器620は、まず、チケット発行サーバ610に対して購入要求データを送信（図37の処理（3）に対応）することで

処理が開始される。ユーザ機器620は、チケット発行サーバ610に対する購入要求データの受信完了のレスポンスを受信すると、ステータスを「購入要求送信完了」に設定し、チケット発行サーバ610からの受信完了のレスポンスを受信できない場合は、処理を中止するか、あるいは同様の処理、ここでは、購入要求送信処理を所定回数繰り返した後、処理を中止し、ステータスを「購入要求送信失敗」とする。ステータスが「購入要求送信完了」である場合にのみ次ステップに進む。

【0269】ステータスが「購入要求送信完了」に遷移すると、次に、ユーザ機器620は、チケット発行サーバ610から、電子チケットを受信（図37の処理

（7）、（8）に対応）し、受信データを検証する。チケット発行サーバ610からのチケットの検証に成功した場合は、ステータスを「電子チケット受信完了」に設定し、データ検証により正当なチケットであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケット受信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット受信失敗」とする。ステータスが「電子チケット受信完了」である場合にのみ次ステップに進む。

【0270】ステータスが「電子チケット受信完了」に遷移した場合、次に、ユーザ機器620は、配信サーバ640に対して、電子チケットを送信（図37の処理（10）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「電子チケット送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、チケット送信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット送信失敗」とする。ステータスが「電子チケット送信完了」である場合にのみ次ステップに進む。

【0271】ステータスが「電子チケット送信完了」に遷移すると、次に、ユーザ機器620は、配信サーバ640から、暗号化コンテンツと、暗号化コンテンツ鍵KpDAS（Kc）を受信し、データ検証（図37の処理（12）、（13）に対応）を実行する。データ検証に成功した場合は、ステータスを「鍵1受信完了」に設定し、データ検証に成功しなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵データの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵1受信失敗」とする。

【0272】ステータスが「鍵1受信完了」に遷移すると、次に、ユーザ機器620は、ユーザ機器認証サーバ630に対して電子チケット（DAS用）と暗号化コンテンツ鍵KpDAS（Kc）を送信（図37の処理（15）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「鍵かけかえ要求送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは

は同様の処理、ここでは、電子チケット（DAS用）と暗号化コンテンツ鍵KpDAS（Kc）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵かけかえ要求送信失敗」とする。ステータスが「鍵かけかえ要求送信完了」である場合にのみ次ステップに進む。

【0273】ステータスが「鍵かけかえ要求送信完了」に遷移すると、次に、ユーザ機器620は、ユーザ機器認証サーバ630から、暗号化コンテンツ鍵KpDEV（Kc）を受信し、データ検証（図37の処理（18）、（19）に対応）を実行する。データ検証に成功した場合は、ステータスを「鍵2受信完了」に設定し、処理を終了する。データ検証に成功しなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵データの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵2受信失敗」とする。

【0274】次にチケット換金サーバ650のステータス遷移について、図52を用いて説明する。チケット換金サーバ650は、電子チケットによる配分権を持つエンティティからの電子チケットを受信（図37の処理（22）、（27）に対応）することで処理が開始される。チケット換金サーバ650は、受信チケットを検証し、検証に成功した場合は、ステータスを「電子チケット受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケットの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット受信失敗」とする。ステータスが「電子チケット受信完了」である場合にのみ次ステップに進む。

【0275】ステータスが「電子チケット受信完了」に遷移すると、次に、チケット換金サーバ650は、電子チケットに基づく換金処理を実行する。換金処理は、予め登録されている利益配分エンティティ、例えば配信サーバを管理するコンテンツプロバイダ（CP）の管理口座、あるいは電子マネー口座等に、電子チケット（CP用）に設定された金額をユーザ機器の管理ユーザの口座から振り替える処理、あるいは既にチケット発行サーバがユーザからの前払い預り金として受領しているチケット発行サーバ管理口座からコンテンツプロバイダ（CP）の管理口座にチケットに設定された金額を振り替える処理として行なわれる。換金処理が完了するとステータスを「換金処理完了」に設定し、換金処理が実行できなかった場合には、処理を中止し、ステータスを「換金処理失敗」とする。

【0276】ステータスが「換金処理完了」に遷移すると、次に、チケット換金サーバ650は、チケットを送信してきたエンティティに対して、換金処理レポートを送信（図37の処理（24）、（29）に対応）し、各エンティティからのデータ受信応答を受信する。データ

受信応答を受信した場合は、ステータスを「換金レポート送信完了」に設定し、処理を終了する。データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、換金レポートの送信処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート送信失敗」とする。チケット換金サーバ650は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【0277】図53にチケット発行体によって発行されるチケットを流通させることによりコンテンツ料金の精算処理を行なう具体的構成例を示す。ユーザ機器802からチケット発行体801に対してコンテンツ購入要求があると、チケット発行体は、コンテンツの取り引きに関する課金処理、電子チケット発行処理を実行する。これらの処理は、例えば予め登録されているユーザ口座、あるいは電子マネー口座等に基づいて設定されるユーザの取り引き金額限度内の電子チケットを発行する処理として実行される。図53に示す例では、コンテンツ購入代金として1,000円分の電子チケットをチケット発行体がユーザ機器に対して発行する。

【0278】図53の例では、コンテンツ料金1000円の配分は、図上部に示すように、チケット発行体としてのショップが販売手数料としてのショップ利益として300円、コンテンツ配信のシステム運営者であるライセンスホルダ（ユーザ機器認証サーバ）803がライセンス料として100円、コンテンツ製作者（配信サーバ）がコンテンツ料として600円を、それぞれ受領する設定であるとする。

【0279】ユーザ機器からの購入要求を受領したチケット発行体801は、コンテンツIDからコンテンツ料金の配分比率の設定情報を求め、複数の料金配分先がある場合は、それぞれの電子チケットを発行する。図53の例では、ライセンスホルダ803に対するライセンス料、100円の配分料金を設定した電子チケットと、コンテンツ製作者に対するコンテンツ料、600円のチケットをユーザ機器802に配信する。配信する電子チケットには、チケット発行体の署名が生成される。

【0280】ユーザ機器802は、ライセンスホルダ803、コンテンツ製作者804それぞれに各電子チケットを送信する。ライセンスホルダ803、コンテンツ製作者804は、受領した電子チケットを検証して、正当なチケットであることを確認した後、銀行（チケット換金サーバ）805にチケットを送信し、換金サーバにおいても署名検証を実行し、正当なチケットであることを確認してそれぞれの配分料金の換金（ex. 振替処理）を行なう。なお、銀行（チケット換金サーバ）において実行するチケットの署名検証は、電子チケットに対して生成されたチケット発行体の署名の検証である。また、チケットに含まれる購入要求データのユーザ機器署名の検証も実行する。

【0281】さらに、チケットの送信主体であるコンテンツ製作者、ライセンスホルダが電子チケットを含む送信データに対して署名を生成し、これらの署名についても銀行（チケット換金サーバ）が署名検証を実行する構成としてもよい。

【0282】図53の構成では、チケット発行体（ショップ）801自身もコンテンツ料金の一部300円分の自己の電子チケットを銀行（チケット換金サーバ）805に送付して換金を行なう構成である。

【0283】これらの各電子チケットの換金処理により、確実にコンテンツ料金の配分が実行される。コンテンツ製作者804は、電子チケットをユーザ機器802から受領して検証した後、コンテンツ鍵Kcで暗号化した暗号化コンテンツと、コンテンツ鍵Kcをライセンスホルダ（ユーザ機器認証サーバ）の公開鍵KpDASで暗号化した暗号化コンテンツ鍵：KpDAS（Kc）をユーザ機器802に送信する。

【0284】ユーザ機器802は、コンテンツ制作者804から受領した暗号化コンテンツ鍵KpDAS（Kc）を電子チケット（DAS）とともに、ライセンスホルダ803に送信する。ライセンスホルダは、電子チケットの検証の後、暗号化コンテンツ鍵KpDAS（Kc）の鍵かけかえ処理を実行し、ユーザ機器の公開鍵KpDEVでコンテンツ鍵を暗号化して、KpDEV（Kc）を生成してユーザ機器802に送信する。ユーザ機器802は、KpDEV（Kc）を自己の秘密鍵KsDEVで復号してコンテンツ鍵Kcを得ることができる。またコンテンツ鍵をデバイスに格納する場合は、自己の保存鍵Kstoで暗号化して保存する。

【0285】上述したように、チケット発行体によって発行するチケットを受信し、正当なチケットであることを条件として配信サーバ（ex. コンテンツ製作者）が暗号化コンテンツと暗号化コンテンツ鍵をユーザ機器に送信し、一方、ライセンスホルダ（ユーザ認証機器）が、同様に電子チケットを受領し、正当なチケットであることを条件として暗号化コンテンツ鍵のかけかえを行なってユーザ機器に配信する構成としたことにより、電子チケットに基づく確実なコンテンツ料金の配分が実行され、ユーザ機器においてコンテンツの利用が可能となる。

【0286】[3. ログ収集サーバによるコンテンツ配信管理] 次に、ユーザ機器がコンテンツの購入を行なった事実をユーザ機器にログとして蓄積し、ログの回収をシステム運営者が行なうことにより、コンテンツの流通実体を正確に把握可能としたコンテンツ配信システムについて説明する。

【0287】図54にログ回収システムを持つコンテンツ配信形態のシステム構成を示す。図54のコンテンツ配信システムは、ユーザ機器に対するコンテンツの配信サービスを行なうショップサーバ（SHOP）901、

ショップサーバ901からのコンテンツ配信を受信するユーザ機器（DEVICE）902、さらに、正当なコンテンツ取り引き管理のためのログ管理サーバとして機能するログ収集サーバ903を主構成要素とし、コンテンツの提供者としてのコンテンツプロバイダ905と、コンテンツプロバイダ905から提供されるコンテンツに対してコンテンツの利用制限情報等の各種情報をヘッダとして生成し、ショップサーバに提供するオーサリングサーバ904、さらに、各エンティティに対して公開鍵証明書（Cert_xxx）を発行する認証局（CA：Certificate Authority）を有する。

【0288】図54の構成において、コンテンツプロバイダ905とオーサリングサーバ904は、ショップサーバ901に対して、流通対象となるコンテンツを提供するエンティティ構成の一例であり、図54の形態に限らず、他の様々な態様でショップサーバに対する流通コンテンツの提供がなされる。例えばコンテンツプロバイダから直接ショップサーバにコンテンツが提供されてもよいし、コンテンツの保持者である著作者から複数のサービスプロバイダを介してショップサーバにコンテンツが提供される場合もある。

【0289】図54の構成例は、本発明の説明の理解を容易にするために、コンテンツ売り上げの一部を取得する権利を持つエンティティの1つの代表例としてコンテンツプロバイダ905を示したものである。図54の構成例では、コンテンツプロバイダ905は、ログ収集サーバ903によって収集されるログに基づいて管理されるコンテンツ売り上げデータの確認により、自己の配分利益を確実に取得することができる。他の利益配分権を有するエンティティがある場合は、そのエンティティが図54の構成に加わり、ログ収集サーバ903によって収集されるログに基づいて自己の配分利益を確認可能である。

【0290】図54の構成において、ショップサーバ901は、図1他の構成において説明したと同様の構成であり、暗号処理、通信処理可能な制御部を有し、コンテンツ取り引き処理に伴うステータス管理を実行して、各機器における取り引き処理シーケンスを実行する。また、コンテンツプロバイダ905とオーサリングサーバ904も暗号処理、通信処理可能な制御部を有し、コンテンツ取り引き処理に伴うステータス管理を実行して、各機器における取り引き処理シーケンスを実行する。

【0291】（ユーザ機器）ユーザ機器902は、先に図7を用いて説明した構成と同様であり、暗号処理、通信処理可能な制御手段230（図7参照）を有する。ただし、本実施例では、制御手段230は、コンテンツ購入処理毎にログデータを生成し、購入管理データベース220中に生成したログデータを格納する。

【0292】ユーザ機器902において生成され格納されるログデータの構成例を図55に示す。図55には、

ログデータの例を2つ示している。(A)構成例1は、ユーザ機器902がショップサーバ901との取り引きにより取得したコンテンツの識別子であるコンテンツID、ユーザ機器の識別子であるユーザ機器ID(ID_DEV)、取り引きを行なったショップの識別子であるショップID(ID_SHOP)、取り引きの日時を示す日付情報が含まれ、これらのデータに対するユーザ機器の署名(Sig. DEV)が生成されている。ログ収集サーバはユーザ機器から受信する購入ログの電子署名の検証処理を実行する。(B)構成例2は、販売確認データとコンテンツの受領日時データに対してユーザ機器の署名(Sig. DEV)が生成された構成である。販売確認データは、ショップサーバ901がユーザ機器902からのコンテンツ購入要求に基づいて生成するコンテンツの販売を実行したことを示すデータである。販売確認データについては、後段でさらに説明する。

【0293】ユーザ機器902は、コンテンツ購入処理に際して、例えば図55に示すログデータを生成しユーザ機器内に格納する。格納されたログデータは、ログ収集サーバ903に送信される。ユーザ機器は自己の公開鍵証明書の更新処理実行時に、その間に蓄積したログデータをログ収集サーバ903に送信する。これらの処理シーケンスについては、フローを用いて後段で詳細に説明する。

【0294】(ログ収集サーバ) ログ収集サーバ903は、図56に示す構成を有する。ログ収集サーバは、収集ログ管理データベース9031を有する。収集ログ管理データベース9031は、様々なユーザ機器から受領するログデータ(図55参照)を格納するデータベースである。

【0295】ログ収集サーバ903は、ユーザ機器902、ショップサーバ901等との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段9032を有する。制御手段9032は、先に説明したショップサーバ等の制御手段と同様、暗号処理手段、通信処理手段としての機能も有する。その構成は、図4を用いて説明した構成と同様である。制御手段9032の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ログ収集サーバ903が格納する暗号鍵等の暗号処理用データとしては、ログ収集サーバ903の秘密鍵:Ks LOG、ログ収集サーバ903の公開鍵証明書Cert__LOG、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局(CA: Certificate Authority)の公開鍵Kp CAがある。

【0296】ログ収集サーバ903は、ユーザ機器902からのログデータ受領と引き換えに、公開鍵証明書の発行手続き処理を実行する。具体的には、ユーザ機器902から更新用の公開鍵を受領して、受領した公開鍵を認証局906に転送して、ユーザ機器の公開鍵証明書の

発行要求を行ない、認証局906の発行した公開鍵証明書を受領してユーザ機器902に送信する。この一連の処理については、フローを用いて後段で詳細に説明する。

【0297】(コンテンツ購入処理) 本実施例における処理は、図54の上段に示すように、

- A. コンテンツ購入処理
- B. ログ送信、公開鍵証明書更新処理
- C. コンテンツ販売準備処理
- D. 売り上げ確認処理

の4つの処理に分類される。以下、これらの各処理についてフローを用いて説明する。

【0298】(A. コンテンツ購入処理) コンテンツ購入処理について、図57、図58のフローを用いて説明する。図57、図58においては、左側にユーザ機器、右側にショップサーバの処理を示している。まず、図57に示すように、処理開始時に、ユーザ機器とショップサーバ間において相互認証が実行される(S1501, S1601)。

【0299】相互認証処理は、図13を用いて説明した公開鍵方式に基づく処理として実行される。この相互認証においては、認証局(CA)906の発行する有効期限の設定された公開鍵証明書をを用いて行われ、ユーザ機器は、有効期限内の公開鍵証明書を持つことが相互認証を成立させるための条件として求められる。後段で説明するが、公開鍵証明書の更新処理は、ログ収集サーバ903に対するログの送信を条件として実行される。

【0300】相互認証処理において生成したセッション鍵(Kses)は、必要に応じて送信データを暗号化してデータ通信を実行したり、あるいはKsesを用いた改竄チェック値(ICV: Integrity Check Value)の生成処理に使用される。ICVの生成については後述する。

【0301】相互認証が成立すると、ユーザ機器は、コンテンツ取り引きにおいて適用するトランザクションIDを例えば乱数に基づいて生成し、購入要求データを生成(S1502)する。購入要求データのフォーマット例を図59(A)に示す。

【0302】購入要求データには前述のトランザクションID(TID_DEV)、コンテンツ識別子であるコンテンツID、ユーザ機器の識別子であるユーザ機器ID(ID_DEV)、コンテンツ価格である表示価格、さらに購入依頼日時を含み、これらのデータに対するユーザ機器の署名(Sig. Dev)を生成した構成である。

【0303】さらに、ユーザ機器は、購入要求データの改竄チェック値(ICV1)を生成して、ショップサーバに送信(S1503)する。改竄チェック値(ICV)は、改竄チェック対象データに対するハッシュ関数を用いて計算され、 $ICV = hash(Kicv, C$

1, C2, ...) によって計算される。KicvはICV生成キーである。C1, C2は改竄チェック対象データの情報であり、改竄チェック対象データの重要情報のメッセージ認証符号(MAC: Message authentication Code)が使用される。

【0304】DES暗号処理構成を用いたMAC値生成例を図60に示す。図60の構成に示すように対象となるメッセージを8バイト単位に分割し、(以下、分割されたメッセージをM1, M2, ..., MNとする)、まず、初期値(Initial Value (以下、IVとする))とM1を排他的論理和する(その結果をI1とする)。次に、I1をDES暗号化部に入れ、鍵(以下、K1とする)を用いて暗号化する(出力をE1とする)。続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する(出力E2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENがメッセージ認証符号(MAC (Message Authentication Code))となる。なお、メッセージとしては、検証対象となるデータを構成する部分データが使用可能である。

【0305】このようなチェック対象データの改竄チェック値(ICV)は、ICV生成キーKicvを用いて生成されたMAC値として構成される。改竄のないことが保証された例えばデータ送信側がデータ生成時に生成したICVと、データ受信側が受信データに基づいて生成したICVとを比較して同一のICVが得られればデータに改竄のないことが保証され、ICVが異なれば、改竄があったと判定される。

【0306】ここでは、ICV生成キーとして相互認証時に生成したセッション鍵: Ksesを使用する。ユーザ機器は、セッション鍵: Ksesを適用して購入要求データ(図59(A)参照)の改竄チェック値(ICV1)を生成して、購入要求データ+ICV1をショップサーバに送信する。

【0307】ショップサーバは、ICV1の検証、すなわち、受信データに基づいてセッション鍵: Ksesを適用して改竄チェック値ICV1'を生成して、受信したICV1=ICV1'が成立するか否かを判定する。成立した場合は、改竄なしと判定する。さらに、ショップサーバは、購入要求データの署名検証(S1603)を行なう。署名検証は、ユーザ機器の公開鍵を用いて行なう。公開鍵はユーザ機器の公開鍵証明書Cert_DEVから取り出されるものであり、有効期限内の公開鍵証明書であることが条件となる。有効期限の切れた公開鍵証明書は、ショップサーバにおいて署名検証に使用されず、購入依頼NGとなる。ICVのチェック、署名検証いずれもOKであれば、ショップサーバは、販売確認データを生成(S1604)する。

【0308】販売確認データは、例えば図59の(B)に示すデータ構成を持つ。ショップサーバの生成したト

ランザクションID(TID_SHOP)、ショップの識別子であるショップID(ID_SHOP)、販売日時、コンテンツ販売に対する運営者手数料情報、ここで運営者とは、例えば、コンテンツ販売システムの管理エンティティ(SH: システムホルダ)であり、図54では、ログ収集サーバ903を管理するエンティティである。

【0309】さらに、CP(コンテンツプロバイダ)売り上げ分配情報、これは、コンテンツの売り上げに対するコンテンツプロバイダの配分を示す情報である。さらに、購入要求データ(図59(A)参照)を含み、これらのデータにショップの署名(Sig. SHOP)が生成された構成である。

【0310】図59(B)の販売確認データフォーマットは、コンテンツの売り上げに対して運営者(SH: システムホルダ)と、コンテンツプロバイダ(CP)との2つのエンティティの配分情報のみを記録しているが、この他にも、コンテンツ売り上げの配分先エンティティが存在する場合は、それらの各エンティティの配分情報も格納する。

【0311】ICVのチェック、署名検証いずれもOKであり、販売確認データを生成(S1604)すると、ショップサーバは購入を承諾するメッセージを含む購入OKデータにセッション鍵Ksesを用いて改竄チェック値(ICV2)を生成付加してユーザ機器に送信(S1605)する。ICVのチェック、署名検証いずれかがNGであると、ショップサーバは購入を拒否するメッセージを含む購入NGデータにセッション鍵Ksesを用いて改竄チェック値(ICV2)を生成付加してユーザ機器に送信(S1606)する。

【0312】さらに、ショップサーバは、購入OKデータをユーザ機器に送信した場合は、販売確認データ(図59(B)参照)と、ヘッダ(コンテンツの利用情報等を含む各種コンテンツ関連情報)に対してセッション鍵Ksesを用いて改竄チェック値(ICV3)を生成したデータとコンテンツとをユーザ機器に送信(S1607)する。

【0313】ユーザ機器は、コンテンツおよび、購入要求応答データ(OKまたはNG)+ICV2を受信(S1504)し、ICV2の検証を行ない、購入要求応答を確認(S1505)する。ICV2によりデータ改竄なしと判定され、購入が受け入れられた(OK)であるときは、販売確認データ(図59(B)参照)と、ヘッダ(コンテンツの利用情報等を含む各種コンテンツ関連情報)+ICV3を受信(S1506)し、ICV3の検証、販売確認データの署名検証を行ないいずれもOKである場合は、コンテンツ受信OKのレスポンスにICV4を生成してショップサーバに送信する。

【0314】ステップS1507の判定がNoである場合は、ステップS1509において、コンテンツ受信N

GのレスポンスにICV4を生成してショップサーバに送信する。

【0315】ショップサーバは、コンテンツ受信OKまたはNG+ICV4を受信（S1608）し、ICV4の検証を行ない（S1611）、さらにユーザ機器からの応答がコンテンツ受信OKである場合は、ユーザに対するコンテンツの課金処理を実行（S1613）する。この課金処理は、前実施例と同様、例えば、ユーザの取り引き口座、あるいはクレジットカード指定口座からコンテンツ料金を受領する処理である。課金処理が終了すると、課金終了メッセージにICV5を生成してユーザ機器に送信（S1614）する。ステップS1611、またはS1612の判定のいずれかがNoである場合は、ステップS1615において課金未了メッセージにICV5を生成してユーザ機器に送信する。

【0316】課金終了（または未了）メッセージ+ICV5を受信したユーザ機器は、ICV5の検証を実行し、さらに課金が無事終了したかを判定し、課金が済んだことを確認すると、購入ログ（図55参照）を生成して自デバイスのメモリに保存の後、コンテンツの利用を行なう。ステップS1512、またはS1513の判定のいずれかがNoである場合は、ステップS1514においてショップサーバから受領したヘッダ、コンテンツを削除する処理を行なう。

【0317】次に、図61、図62を用いてユーザ機器と、ログ収集サーバ間で行われる鍵更新処理と、ログ送信処理とについて説明する。図61、図62の左側にユーザ機器の処理、右側にログ収集サーバの処理を示す。この処理は、コンテンツをショップサーバから購入するユーザ機器がユーザ機器に格納されたユーザ機器の公開鍵証明書を更新する際に実行される。ユーザ機器の公開鍵証明書には有効期限が設定されており、一定期間毎に更新処理を実行することが必要となる。図61の処理から説明する。

【0318】まず、ユーザ機器とログ収集サーバは、相互認証を実行（S1521、S1721）しセッション鍵の生成を行なう。ユーザ機器は認証成立を条件として、ユーザ機器デバイス内のメモリに格納された購入ログを取り出して、購入ログに対してセッション鍵Ksesで改竄チェック値（ICV1）を生成して購入ログ+ICV1をログ収集サーバに送信（S1522）する。

【0319】ログ収集サーバは、購入ログ+ICV1を受信（S1722）し、ICV1の検証を実行（S1723）し、検証OKの場合は、ログをデータベース内に保存（S1724）する。なお、ログ収集サーバは、さらに、購入ログ中のユーザ機器の電子署名の検証処理を行なって、データ改竄の有無を更にチェックする構成としてもよい。ログ収集サーバは、さらに、ログ受信OKデータにセッション鍵Ksesで改竄チェック値（ICV2）を生成し、ログ受信OKデータ+ICV2をユーザ機器に送信（S1725）する。ステップS1723

のICV1の検証NGであったときは、ログ受信NGデータにセッション鍵Ksesで改竄チェック値（ICV2）を生成し、ログ受信NGデータ+ICV2をユーザ機器に送信（S1726）する。

【0320】ユーザ機器は、ログ受信データ+ICV2を受信（S1523）し、ICV2の検証OK、ログ受信OK（S1524）である場合は、更新用の公開鍵（KpDEV）と秘密鍵（KsDEV）のペアを生成（S1525）し、生成した公開鍵（KpDEV）に改竄チェック値（ICV3）を生成付加してログ収集サーバに送信（S1526）する。

【0321】ログ収集サーバは、公開鍵（KpDEV）+ICV3をユーザ機器から受信する（S1727）と、ICV3の検証を実行（S1731）し、検証OKである場合は公開鍵受信OKメッセージに対するICV4を生成付加してユーザ機器に送信（S1732）する。ICV3の検証がNGである場合は公開鍵受信NGメッセージにICV4を生成付加してユーザ機器に送信（S1733）する。

【0322】さらに、ログ収集サーバは、公開鍵受信OKメッセージに対するICV4を生成付加してユーザ機器に送信（S1732）した場合、発行局（CA）に対して受領公開鍵とともに、公開鍵証明書の発行を要求して、ユーザ機器の更新された公開鍵証明書（Cert_DEV）を取得（S1734）し、さらに、更新された公開鍵証明書（Cert_DEV）に対する改竄チェック値ICV5を生成付加してユーザ機器に送信（S1735）する。

【0323】ユーザ機器は、公開鍵受信結果（OKまたはNG）+ICV4を受信した後、ICV4の検証を行ない、ICV4検証OKであり、公開鍵受信OK（S1532）である場合には、更新された公開鍵証明書+ICV5の受信（S1533）を実行し、ICV5の検証、受信した公開鍵証明書の検証（S1534）を実行する。いずれの検証もOKである場合は、公開鍵証明書内の公開鍵を取り出して、自己の送信した公開鍵との比較（S1535）を行ない、一致した場合は更新用に生成した秘密鍵、および受領した公開鍵証明書をユーザ機器内のメモリに保存（S1536）し、ログ（ログ収集サーバに送付済みのログ）の消去処理（S1537）を実行する。

【0324】ステップS1532、S1534、S1535のいずれかの判定がNoである場合は、有効な公開鍵証明書の更新処理は実行されず、処理は終了する。

【0325】次に、コンテンツプロバイダとログ収集サーバ間で実行されるコンテンツ売り上げ確認処理について図63のフローに基づいて説明する。ログ収集サーバは、ユーザ機器から受領する購入ログに基づいてコンテンツ料金の1または複数の料金受領エンティティに対す

る料金配分情報を管理し、料金受領エンティティからの売り上げ確認要求に応じて料金配分情報に基づく応答処理を実行する。ログ収集サーバは、購入ログに含まれるコンテンツIDと予めログ収集サーバが保有するコンテンツ料金配分情報から、コンテンツの売り上げに基づく料金受領エンティティの売り上げを算出することができる。なお、図55(B)に示す販売確認データを格納したログを受領する構成である場合は、販売確認データに含まれる分配情報に基づいて料金受領エンティティの売り上げを算出することができる。

【0326】まず、コンテンツプロバイダとログ収集サーバ間において、相互認証(S1521, S1721)が実行され、セッション鍵 K_{ses} が生成される。ログ収集サーバは、相互認証の成立を条件として、コンテンツプロバイダ(CP)の公開鍵証明書 $Cert_CP$ からコンテンツプロバイダの識別子 ID_CP を取り出し(S1722)、 ID_CP に対応する売り上げデータをデータベースに格納したログ情報に基づいて生成(S1723)する。収集したログデータには、前述したようにコンテンツプロバイダの配分情報が格納されており、ログデータに基づいて各コンテンツプロバイダの配分料金が求められる。さらに、ログ収集サーバは、売り上げデータに対する改竄チェック値 $ICV1$ を生成付加してコンテンツプロバイダ(CP)に送信(S1724)する。

【0327】コンテンツプロバイダ(CP)は、ログ収集サーバから売り上げデータ+ $ICV1$ を受信(S1522)し、 $ICV1$ の検証を行なってデータ改竄のないことを確認して(S1523)売り上げデータをメモリに保存(S1524)する。 $ICV1$ の検証を行なってデータ改竄ありの場合は、メモリに対するデータ保存を実行せず、処理を終了する。この場合は、再度、ログ収集サーバに対する売り上げデータ要求を行なう。

【0328】次に、ショップサーバとログ収集サーバ、コンテンツプロバイダ間で実行される売り上げ報告処理について図64、図65の処理フローに基づいて説明する。ショップサーバは、コンテンツの売り上げデータを管理し、ログ収集サーバに対して、所定期間内の全売り上げてデータまたは、料金受領エンティティ毎の売り上げデータを送信する処理を実行する。図64は、ショップサーバが実行したコンテンツ販売処理全体の売り上げを一括してログ収集サーバに送信する処理であり、図65の処理は、ショップサーバが実行したコンテンツ販売処理中、特定のコンテンツプロバイダの提供したコンテンツに関する売り上げを選択してコンテンツプロバイダに送信する処理である。

【0329】図64の売り上げ一括報告処理から説明する。まず、ショップサーバとログ収集サーバ間において、相互認証(S1631, S1731)が実行され、セッション鍵 K_{ses} が生成される。ショップサーバ

は、相互認証の成立を条件として、所定期間の全売り上げデータをデータベースから取り出し、全売り上げデータに対する改竄チェック値 $ICV1$ を生成付加してログ収集サーバに送信(S1632)する。

【0330】ログ収集サーバは、ショップサーバから全売り上げデータ+ $ICV1$ を受信(S1732)し、 $ICV1$ の検証を行なってデータ改竄のないことを確認して(S1733)、売り上げデータをメモリに保存(S1734)する。 $ICV1$ の検証を行なってデータ改竄ありの場合は、メモリに対するデータ保存を実行せず、処理を終了する。この場合は、再度、ショップサーバに対する売り上げデータ要求を行なう。

【0331】図65の特定コンテンツプロバイダ売り上げ報告処理について説明する。まず、ショップサーバとコンテンツプロバイダ間において、相互認証(S1641, S1741)が実行され、セッション鍵 K_{ses} が生成される。ショップサーバは、相互認証の成立を条件として、相互認証で得られたコンテンツプロバイダの公開鍵証明書 $Cert_CP$ からコンテンツプロバイダの識別子である ID_CP を取り出し(S1642)、取り出した ID_CP に基づいて、売り上げデータの検索を行ない、その特定コンテンツプロバイダの提供コンテンツの売り上げデータを取得(S1643)する。さらに売り上げデータに対する改竄チェック値 $ICV1$ を生成付加してログ収集サーバに送信(S1644)する。

【0332】ログ収集サーバは、ショップサーバから全売り上げデータ+ $ICV1$ を受信(S1742)し、 $ICV1$ の検証を行なってデータ改竄のないことを確認して(S1743)、売り上げデータをメモリに保存(S1744)する。 $ICV1$ の検証を行なってデータ改竄ありの場合は、メモリに対するデータ保存を実行せず、処理を終了する。この場合は、再度、ショップサーバに対する売り上げデータ要求を行なう。

【0333】本実施例の構成によれば、ユーザ機器の公開鍵証明書の更新処理に応じてコンテンツ購入ログデータを収集することが可能となり、ログ収集サーバを管理するシステム運営者(SH: System Holder)は、コンテンツ売り上げ状況を確実に把握することが可能となる。ユーザ機器の公開鍵証明書は、ショップサーバとの相互認証処理において必要であり、有効な期限の設定された公開鍵証明書を有することがコンテンツ購入を実行するための条件となる。また、ユーザ機器からの購入要求データ等に付加される署名の検証もユーザ機器の公開鍵証明書から取り出される公開鍵によって実行されることになり、有効な期限の設定された公開鍵証明書を有することが署名検証においても必要となる。従って、ユーザ機器は、コンテンツ購入を行なうためには、ログデータをログ収集サーバに送信し、公開鍵証明書の更新を行ない有効な期限を持つ公開鍵証明書を有することが必要となる。公開鍵証明書の有効期限を例えば1ヶ月、また

は3ヶ月等に設定することにより、ログ収集サーバを管理するシステム運営者（SH：System Holder）は、各設定機関毎の蓄積ログを確実に収集することができる。

【0334】上述したように、システム運営者の管理するログ収集サーバにより確実にユーザ機器からのログデータが収集され、コンテンツ売り上げ状況を管理することが可能となる。さらに、ログデータ中の売り上げ配分情報に基づいて、コンテンツ売り上げをコンテンツプロバイダ等の売り上げ利益取得権利者に対して正確な配分が可能となる。

【0335】また、本実施例では、各エンティティ間において通信されるデータに相互認証時に生成したセッション鍵 *Session Key* を改竄チェック値（ICV）の生成鍵として用い、送信データにICVを付加して通信する構成としたので、通信データの安全性がさらに高まることになる。

【0336】なお、上述した実施例では、ユーザ機器とショップサーバ間の相互認証処理、署名生成、署名検証処理のいずれも実行する構成として説明したが、いずれかのみ処理、すなわち、相互認証のみ、あるいは署名生成、署名検証処理のみを実行する構成として、いずれかにおいて有効期限内の公開鍵証明書の利用を必須とする構成としてもよい。

【0337】〔4. 属性データを記録した公開鍵証明書または属性証明書利用構成〕次に、属性データを記録した公開鍵証明書または属性証明書の利用構成について説明する。例えば上述したコンテンツ配信構成において、悪意のショップ運営者がユーザ機器になりすましてコンテンツの架空取引引きを実行したり、あるいはコンテンツプロバイダとショップ間における架空コンテンツ取引引きを行なう可能性がある。また、正当な取引引きを実行しようとするユーザ機器がショップサーバであると信じて通信を開始し、ショップサーバ相手のコンテンツ購入要求を実行して、例えばクレジット口座番号の送信処理を実行するような場合、相手がショップサーバになりすました不正なサーバであるような場合は、ユーザ機器からクレジット口座番号を不正に取得する等の処理が実行されるおそれがある。さらに、ユーザ機器がショップになりすまして、他のユーザ機器に対してコンテンツの架空販売を行なうなどの処理を行なう可能性も否定できない。このような事態が発生すると、システム運営者は正確なコンテンツ配信実体を把握することが困難となる。

【0338】このような正規なコンテンツ配信ルート以外の架空取引等を防止する構成として、以下、属性データを記録した公開鍵証明書または属性証明書利用構成を説明する。

【0339】属性データとは、ユーザ機器（DEVICE）、ショップ（SHOP）、コンテンツプロバイダ（CP）、サービス運営者（SH）、公開鍵証明書、属

性証明書の発行審査を行なう登録局等、コンテンツ配信システムを構成するエンティティの種別を識別するデータである。

【0340】属性データの構成例として、属性データの内容を示すテーブルを図66に示す。図66に示すように、異なるコードが各エンティティに割り当てられる。例えば、ユーザ機器あるいはショップ等から公開鍵証明書、属性証明書の発行要求を受けつけ、審査を行なう登録局には「0000」、コンテンツ配信システム上で流通するコンテンツに対するライセンスを徴収するシステムホルダとしてのサービス運営者には「0001」が属性コードとして割り振られる。上述した例では、サービス運営者は鍵かけかえ処理を実行するユーザ機器認証サーバを管理するエンティティであったり、また、ログ情報を収集するログ情報収集サーバを管理するエンティティである。

【0341】さらに、ユーザ機器に対してコンテンツを販売するショップとしてのコンテンツ販売者には、「0002」、ショップ（コンテンツ販売者）からの要求に応じてコンテンツをユーザに配信する配信サーバの運営エンティティであるコンテンツ配信者には、「0003」、コンテンツを購入し利用するユーザ機器には「0004」のコードが割り当てられる。この他にもコンテンツ配信に係わるエンティティに対して、その種類に応じて異なるコードが割り当てられる。なお、ショップに必ずしも1つのコードを割り当てる構成に限らず、役割、機能の異なるショップがある場合には、異なるコードを割り当てて、それぞれを区別可能にしてもよいし、またユーザ機器にも、何らかのカテゴリに応じて異なる属性コードを割り当てる構成としてもよい。

【0342】上述した属性情報は、公開鍵証明書に含める構成と、公開鍵証明書とは異なる属性証明書を発行し、属性証明書によって属性を識別する構成とがある。属性情報を持つ公開鍵証明書の構成例を図67に示す。

【0343】図67に示す公開鍵証明書は、証明書のバージョン番号、公開鍵証明書発行局（CA）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、発行局の名前、証明書の有効期限、証明書利用者の名前（ex. ユーザ機器ID）、証明書利用者の公開鍵、さらに、上述した【0000】、【0001】…【nnnn】等の属性情報、さらに電子署名を含む。証明書の通し番号は、例えば発行年（4バイト）、月（2バイト）、日（2バイト）、シリアル番号（8バイト）の合計16バイトとする。利用者名は、登録局の定める識別可能な名前、あるいは乱数、通し番号を用いてもよい。あるいは上位バイトをカテゴリとし、下位バイトを通し番号とする構成としてもよい。

【0344】電子署名は、証明書のバージョン番号、公開鍵証明書発行局（CA）が証明書利用者に対し割り付

ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、発行局の名前、証明書の有効期限、証明書利用者の名前、証明書利用者の公開鍵、並びに属性データ全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して発行局の秘密鍵を用いて生成したデータである。

【0345】公開鍵証明書発行局（CA）は、図67に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。

【0346】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する発行局の公開鍵 K_{pCA} を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局の公開鍵を保持している必要がある。

【0347】次に図68に属性情報を持たない公開鍵証明書と、属性証明書のデータ構成を示す。（A）は属性情報を持たない公開鍵証明書であり、図67に示す公開鍵証明書から属性情報を取り除いたデータ構成であり、公開鍵証明書発行局が発行する。（B）は属性証明書である。属性証明書は、属性証明書発行局（AA：Attribute Authority）が発行する。

【0348】図68に示す属性証明書は、証明書のバージョン番号、属性証明書発行局（AA）が発行する属性証明書に対応する公開鍵証明書の通し番号、これは対応公開鍵証明書の証明書の通し番号と同一であり、両証明書を関連づけるリンクデータとしての機能を持つ。属性証明書によって通信相手の属性を確認しようとするエンティティは、公開鍵証明書とリンクする属性証明書を、公開鍵証明書および属性証明書に共通に格納された公開鍵証明書通し番号に基づいて確認し、公開鍵証明書と同一の公開鍵証明書通し番号を格納した属性証明書から属性情報を取得することができる。通し番号は、例えば発行年（4バイト）、月（2バイト）、日（2バイト）、シリアル番号（8バイト）の合計16バイトとする。さらに、電子署名に用いたアルゴリズムおよびパラメータ、属性証明書発行局の名前、証明書の有効期限、証明書利用者の名前（ex. ユーザ機器ID）、これは、対応する公開鍵証明書の利用者名と同一であり、登録局の定める識別可能な名前、あるいは乱数、通し番号、あるいは上位バイトをカテゴリとし、下位バイトを通し番号としたデータ構成である。さらに、上述した【0000】、【0001】…【nnnn】等の属性情報、属性証明書発行局（AA）の電子署名を含む。

【0349】電子署名は、証明書のバージョン番号、公開鍵証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、発行局の名前、証明書の有効期限、

証明書利用者の名前、並びに属性データ全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して属性証明書発行局の秘密鍵を用いて生成したデータである。

【0350】属性証明書発行局（AA）は、図68

（B）に示す属性証明書を発行するとともに、有効期限が切れた属性証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。

【0351】図69にコンテンツ取り引きに参加するユーザ機器、ショップサーバがそれぞれ使用する公開鍵証明書を新規に発行する手続きを説明する図を示す。なお、ここでショップサーバ1010、ユーザ機器1020は、前述の図1他で説明したと同様の構成を持つ。サービス運営体1030は、コンテンツ配信全体を管理するシステムホルダ（SH）であり、前述したコンテンツ鍵のかけかえ処理、あるいはユーザ機器のコンテンツ購入により生成されるログを収集する等の手法により、コンテンツの流通状況を把握する。ここでは、さらに、ショップサーバ1010、ユーザ機器1020他の公開鍵証明書および属性証明書の発行要求の受付、審査を実行する登録局（RA：Registration Authority）としての機能も兼ね備える。なお、本例ではサービス運営体1030がシステムホルダ（SH）としての機能と、登録局（RA）としての機能を持つ構成であるが、これらは別々の独立したエンティティとして構成してもよい。

【0352】図69では、ユーザ機器1020における公開鍵証明書の新規発行手続きをA1～A8で示し、ショップサーバ1010の公開鍵証明書の新規発行手続きをB1～B7で示している。まず、ユーザ機器1020における公開鍵証明書の新規発行手続きについて説明する。

【0353】（A1）相互認証

まず、ユーザ機器1020は、サービス運営体1030との間で相互認証を実行する。ただし、この時点でユーザ機器1020は、公開鍵証明書を保有していないので、公開鍵証明書をを用いた相互認証を実行することはできず、先に図12を用いて説明した対称鍵暗号方式、すなわち、共有秘密鍵、識別子（ID）を用いた相互認証処理を実行（詳細は図12に関する説明を参照）する。

【0354】（A2）公開鍵、秘密鍵ペア生成

（A3）公開鍵証明書発行要求

（A4）審査&公開鍵証明書発行要求

（A5）公開鍵証明書発行要求

相互認証が成立すると、ユーザ機器1020は、自己のデバイス内の暗号処理部において、新規に登録する公開鍵と秘密鍵のペアを生成し、生成した公開鍵をサービス運営体1030に対して、証明書発行要求とともに送信する。公開鍵証明書発行要求を受信したサービス運営体1030は、発行要求を審査し、公開鍵証明書を発行す

るエンティティとしての要件を満足している場合に、証明書発行要求を公開鍵証明書発行局（CA）1040に対して送信する。なお、ここで発行する公開鍵証明書が図68（A）に示す属性情報を持つ公開鍵証明書である場合は、サービス運営体1030は、証明書発行要求を送信してきたエンティティの属性をIDに基づいて判定する。

【0355】コンテンツ配信に参加するユーザ機器には、予めユーザ機器識別子（ID）および秘密情報としての秘密鍵が格納され、これらユーザ機器ID、秘密鍵はサービス運営体1030によって管理された構成であり、サービス運営体1030は、ユーザ機器から送信されるIDに基づき秘密情報格納データベースを検索し、予め登録済みのユーザ機器IDであることを確認した後、秘密鍵を取り出し、この鍵を用いてユーザ機器と図12に基づく相互認証を行ない、相互認証に成功した場合にのみコンテンツ配信に参加可能なユーザ機器であることを確認する。

【0356】（A6）公開鍵証明書発行

（A7）公開鍵証明書送信

（A8）公開鍵証明書送信

サービス運営体1030からの公開鍵証明書発行要求を受信した公開鍵証明書発行局1040は、ユーザ機器の公開鍵を格納し、公開鍵証明書発行局1040の電子署名を持つ公開鍵証明書（図67または図68（A））を発行し、サービス運営体1030に送信する。サービス運営体1030は、公開鍵証明書発行局1040から受信した公開鍵証明書をユーザ機器1020に対して送信する。ユーザ機器は、受信した公開鍵証明書と先ほど

（A2）で生成しておいた秘密鍵を自デバイス内に格納し、コンテンツ取り引きの際の相互認証、データ暗号化、復号処理等に使用可能となる。

【0357】一方、ショップサーバ1010の公開鍵証明書の発行手続きは、基本的にユーザ機器における証明書発行手続きと同様であるが、ショップサーバは、コンテンツの販売を手がけるエンティティとしてサービス運営体1030に認可してもらう手続きが必要となる。従って、ショップサーバ1010は、自己の公開鍵とともに、ライセンス申請（図69、B2の手続き）を実行することが必要となる。これは、例えばサービス運営体1030が定めるポリシーに従ったコンテンツ販売を実行することをショップサーバ1010が受諾する処理として実行されるものである。サービス運営体1030は、ショップサーバ1010がサービス運営体1030が定めるポリシーに従ったコンテンツ販売を実行可能であり、ショップサーバ1010がポリシーを遵守することを受諾した場合には、ショップに対する公開鍵証明書の発行手続きを進める。公開鍵証明書の発行手続き処理は、上述したユーザ機器の場合と同様である。

【0358】次に、公開鍵証明書の更新処理について図

70を用いて説明する。公開鍵証明書は図67、図68（A）に示すように有効期限が定められており、公開鍵証明書を使用するエンティティは有効期限のすぎた証明書は使用できないので、有効期限内に更新処理を実行し、新たな有効期限の設定された公開鍵証明書の発行手続きを行なうことが必要となる。

【0359】図70において、ユーザ機器1020における公開鍵証明書の更新手続きをA1～A8で示し、ショップサーバ1010の公開鍵証明書の更新手続きをB1～B7で示している。まず、ユーザ機器1020における公開鍵証明書の更新手続きについて説明する。

【0360】（A1）相互認証

まず、ユーザ機器1020は、サービス運営体1030との間で相互認証を実行する。この時点でユーザ機器1020は、現在有効な公開鍵証明書を保有しているので、公開鍵証明書を用いた相互認証を実行する。これは先に図13を用いて説明した相互認証処理である。なお、すでに手持ちの公開鍵証明書の有効期限がすぎている場合は、新規発行手続きと同様先に図12を用いて説明した共有秘密鍵、識別子（ID）を用いた相互認証処理を実行するようにしてもよい。

【0361】（A2）新規公開鍵、秘密鍵ペア生成

（A3）公開鍵証明書更新要求

（A4）審査&公開鍵証明書更新要求

（A5）公開鍵証明書更新要求

相互認証が成立すると、ユーザ機器1020は、自己のデバイス内の暗号処理部において、更新用の新規公開鍵と秘密鍵のペアを生成し、生成した公開鍵をサービス運営体1030に対して、証明書更新要求とともに送信する。公開鍵証明書更新要求を受信したサービス運営体1030は、更新要求を審査し、更新要件を満足している場合に、証明書更新要求を公開鍵証明書発行局（CA）1040に対して送信する。なお、ここで発行する公開鍵証明書が図68（A）に示す属性情報を持つ公開鍵証明書である場合は、サービス運営体1030は、証明書発行要求を送信してきたエンティティの属性をIDに基づいて判定する。

【0362】（A6）公開鍵証明書更新

（A7）公開鍵証明書送信

（A8）公開鍵証明書送信

サービス運営体1030からの公開鍵証明書更新要求を受信した公開鍵証明書発行局1040は、ユーザ機器の新規公開鍵を格納し、公開鍵証明書発行局1040の電子署名を持つ公開鍵証明書（図67または図68

（A））を発行し、サービス運営体1030に送信する。サービス運営体1030は、公開鍵証明書発行局1040から受信した公開鍵証明書をユーザ機器1020に対して送信する。ユーザ機器は、受信した公開鍵証明書と先ほど（A2）で生成しておいた秘密鍵を自デバイス内に格納し、コンテンツ取り引きの際の相互認証、デ

ータ暗号化、復号処理等に使用可能となる。

【0363】一方、ショップサーバ1010の公開鍵証明書の更新手続きは、基本的にユーザ機器における証明書更新手続きと同様であるが、前述のライセンス申請の更新(図70、B2の手続き)を実行することが必要となる。サービス運営体1030が、ショップサーバ1010のライセンス更新を認めた場合には、ショップに対する公開鍵証明書の更新手続きを進める。公開鍵証明書の更新手続き処理は、上述したユーザ機器の場合と同様である。

【0364】次に、図71を用いて属性証明書の新規発行手続きについて説明する。属性証明書は、図68

(B)に示す証明書であり、図68(A)に示す公開鍵証明書の発行の後、属性証明書が発行される。図71では、ユーザ機器1020における属性証明書の新規発行手続きをA1~A7で示し、ショップサーバ1010の公開鍵証明書の新規発行手続きをB1~B7で示している。まず、ユーザ機器1020における公開鍵証明書の新規発行手続きについて説明する。

【0365】(A1)相互認証

まず、ユーザ機器1020は、サービス運営体1030との間で相互認証を実行する。この時点でユーザ機器1020は、すでに公開鍵証明書発行局公開鍵証明書を保有しているので、公開鍵証明書をを用いた相互認証を実行する。

【0366】(A2)属性証明書発行要求

(A3)審査&属性証明書発行要求

(A4)属性証明書発行要求

相互認証が成立すると、ユーザ機器1020は、サービス運営体1030に対して、属性証明書発行要求を送信する。属性証明書発行要求を受信したサービス運営体1030は、発行要求を審査し、属性証明書を発行するエンティティとしての要件を満足している場合に、証明書発行要求を属性証明書発行局(AA)1050に対して送信する。なお、ここでサービス運営体1030は、証明書発行要求を送信してきたエンティティの属性をIDに基づいて判定する。前述したように、コンテンツ配信に参画するユーザ機器には、予めユーザ機器識別子(ID)が格納され、これらユーザ機器IDはサービス運営体1030によって管理された構成であり、サービス運営体1030は、ユーザ機器から送信されるIDと、予め登録済みのユーザ機器IDと比較参照することにより、コンテンツ配信に参画可能なユーザ機器であることを確認する。

【0367】(A5)属性証明書発行

(A6)属性証明書送信

(A7)属性証明書送信

サービス運営体1030からの属性証明書発行要求を受信した属性証明書発行局1050は、ユーザ機器の属性情報を格納し、属性証明書発行局1050の電子署名を

持つ属性証明書(図68(B))を発行し、サービス運営体1030に送信する。サービス運営体1030は、属性証明書発行局1050から受信した属性証明書をユーザ機器1020に対して送信する。ユーザ機器は、受信した属性証明書を自デバイス内に格納し、コンテンツ取り引きの際の属性確認処理に使用する。

【0368】一方、ショップサーバ1010の属性証明書の発行手続き(B1~B7)は、基本的にユーザ機器における証明書発行手続きと同様である。また、属性証明書の更新手続きも新規発行手続きと同様の手続きとなる。

【0369】次に、属性証明書による属性確認処理、または公開鍵証明書に格納された属性情報による属性確認処理を伴うコンテンツ取り引きについて説明する。

【0370】図72に相互認証時に併せて属性確認処理を実行する処理構成を示す。図72の構成は、先に説明した図1のシステム構成と同様である。すなわち、コンテンツの販売を実行するショップサーバ1010、コンテンツ購入を実行するユーザ機器1020、ユーザ機器認証サーバ1030を構成要素とする。ここで、ユーザ機器認証サーバ1030は、前述したサービス運営体の管理下にある。図72の番号(1)から(20)の順に処理が進行する。各番号順に処理の詳細を説明する。

【0371】(1)相互認証および属性確認処理
コンテンツをショップサーバ1010から購入しようとするユーザ機器1020は、ショップサーバとの間で相互認証処理を行なう。データ送受信を実行する2つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が1つの好ましいデータ転送方式である。公開鍵方式の相互認証処理は、公開鍵証明書の発行局の署名検証の後、相手型の公開鍵を取り出して実行される。詳細は前述の図13に関する説明を参照されたい。

【0372】さらに、本実施例においては、属性確認処理を実行する。ショップサーバ1010は、通信相手の公開鍵証明書に属性データが格納されている場合は、その属性がユーザ機器であることを示すデータであることを確認する。公開鍵証明書に属性データが格納されていない場合は、属性証明書をを用いて属性の確認を行なう。属性証明書には、属性証明書発行局の秘密鍵を用いて署名がなされているので、属性証明書発行局の公開鍵:KpAAを用いて署名検証を実行し、正当な証明書であることを確認し、属性証明書の「通し番号」および/または「利用者(ID)」が、公開鍵証明書内の「通し番号」および/または「利用者(ID)」と一致しているか確認した後、証明書内の属性情報を確認する。

【0373】一方、ユーザ機器1020は、通信相手の公開鍵証明書に属性データが格納されている場合は、その属性がショップであることを示すデータであることを確認する。公開鍵証明書に属性データが格納されていない場合は、属性証明書について、属性証明書発行局の公開鍵：KpAAを用いて署名検証を実行し、正当な証明書であることを確認し、属性証明書の「通し番号」および／または「利用者（ID）」が、公開鍵証明書内の「通し番号」および／または「利用者（ID）」と一致しているか確認した後、証明書内の属性情報を確認する。

【0374】ショップサーバ1010は、コンテンツ購入要求主体の公開鍵証明書または属性証明書の属性がユーザ機器であることを確認し、ユーザ機器1020は、コンテンツ購入要求先の公開鍵証明書または属性証明書の属性がショップであることを確認して、その後の処理に移行する。

【0375】属性確認処理のフローを図73に示す。図73（A）は、公開鍵証明書に属性データが格納されている場合の公開鍵証明書を用いた属性確認処理であり、（B）は、属性証明書を用いた属性確認処理である。

【0376】図73（A）のフローから説明する。まず、ステップS2101において、公開鍵証明書を用いた相互認証処理を実行（図13参照）し、認証が成立したことを条件として（S2102の判定Yes）、相手の公開鍵証明書から属性情報を取り出す。属性情報が正当である場合に（S2104の判定Yes）、相互認証、属性確認が成功したものと判定（S2105）し、その後の処理に移行する。なお、属性が正当であるとは、例えばユーザ機器がショップサーバにアクセスしコンテンツ購入要求を実行しようとしている場合は、属性がショップであれば正当であると判定し、ショップ以外の例えば他のユーザ機器を示す属性コードであれば正当でないと判定する。この判定処理は、例えばショップサーバに対してコンテンツ購入要求を実行する場合は、コンテンツ購入要求処理シーケンス（ex. 実行プログラム）中に属性コード比較処理を実行するステップを含ませ、予めショップに対して付与されたコード【0002】と、通信相手（エンティティ）の公開鍵証明書、または属性証明書から取得した属性コードとを比較し、一致すれば正当と判定し、不一致であれば正当でないと判定する。あるいは、通信相手（エンティティ）の公開鍵証明書、または属性証明書から取得した属性コードをディスプレイに表示するなどして、通信相手として想定したエンティティに設定された属性コードとを比較してユーザ自身が判定する構成としてもよい。ステップS2102、S2104で判定がNoの場合は、相互認証、属性確認が失敗であると判定（S2106）し、その後の処理を中止する。

【0377】属性正当性の判定は、上述のように、ショ

ップに対する処理実行プログラムでは、予めショップに対して付与されたコード【0002】と、通信相手（エンティティ）の公開鍵証明書、または属性証明書から取得した属性コードとを比較する処理としてステップが実行され、また、ユーザ機器がユーザ機器認証サーバに対して実行する例えば鍵かけかえ要求処理実行シーケンス（ex. プログラム）では、予めユーザ機器認証サーバに対して付与されたコード【0001】と、通信相手（エンティティ）の公開鍵証明書、または属性証明書から取得した属性コードとを比較する処理としてステップが実行される。その他、ショップとユーザ機器認証サーバ間における通信処理においても、それぞれのエンティティで通信相手を特定して実行する処理シーケンス（ex. プログラム）において、予め正当な通信相手として設定された属性コードと、通信相手（エンティティ）の公開鍵証明書、または属性証明書から取得した属性コードとを比較する処理としてステップが実行される。

【0378】次に、図73（B）の属性証明書を適用したフローについて説明する。まず、ステップS2201において、公開鍵証明書を用いた相互認証処理を実行（図13参照）し、認証が成立したことを条件として（S2202の判定Yes）、相手の属性証明書の検証を属性証明書発行局の公開鍵を用いて実行（S2203）し、検証が成功し、公開鍵証明書とリンクする属性証明書を、公開鍵証明書および属性証明書に共通に格納された公開鍵証明書通し番号に基づいて確認した（S2204の判定Yes）ことを条件として、公開鍵証明書と同一の公開鍵証明書通し番号を格納した属性証明書から属性情報を取り出す（S2205）。属性情報が正当である場合に（S2206の判定Yes）、相互認証、属性確認が成功したものと判定（S2207）し、その後の処理に移行する。ステップS2202、S2204、S2206で判定がNoの場合は、相互認証、属性確認が失敗であると判定（S2208）され、その後の処理は中止される。

【0379】（2）トランザクションID、購入要求データ生成、および

（3）購入要求データ送信

上述のショップサーバ1010とユーザ機器1020間の相互認証および属性確認が成功すると、ユーザ機器1020は、コンテンツの購入要求データを生成する。購入要求データの構成は、先に説明した図14（a）に示す構成であり、コンテンツ購入の要求先であるショップサーバ1010の識別子であるショップID、取り引きの識別子として、ユーザ機器1020の暗号処理手段が乱数に基づいて生成するトランザクションID、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツIDの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。

【0380】（4）受信データ検証

図14 (a) に示す購入要求データをユーザ機器1020から受信したショップサーバは、受信データの検証処理を実行する。検証処理は、先に、図15を用いて説明したように、ユーザ機器の公開鍵証明書Cert_DEVの検証の後、公開鍵証明書からユーザ機器の公開鍵: KpDEVを取り出して、ユーザ機器の公開鍵: KpDEVを用いて購入要求データのユーザ機器署名の検証を行なうものである。

【0381】検証がOK、すなわち購入要求データの改竄がないと判定されると、受信データが正当なコンテンツ購入要求データであると判定される。検証が不成立の場合は、購入要求データが改竄ありと判定され、その購入要求データに対する処理が中止される。

【0382】(5) 暗号化コンテンツおよび暗号化コンテンツ鍵データ1 (ショップ) 送信

ショップサーバ1010において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定すると、ショップサーバ1010は、暗号化コンテンツおよび暗号化コンテンツ鍵データ1 (ショップ) をユーザ機器に送信する。これらは、いずれもコンテンツデータベースに格納されたデータであり、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ: Kc (content) と、コンテンツキー: Kcをユーザ機器認証サーバ (DAS) 1030の公開鍵で暗号化した暗号化コンテンツ鍵データ: KpDAS (Kc) である。

【0383】暗号化コンテンツ鍵データ1 (ショップ) は、先に説明した図14 (b) に示す構成である。すなわち、コンテンツ購入の要求元であるユーザ機器1020の識別子であるユーザ機器ID、購入要求データ (図14 (a) のユーザ機器公開鍵証明書を除いたデータ)、コンテンツ取り引きに伴いショップサーバ1010が生成したショップ処理No.、暗号化コンテンツ鍵データ: KpDAS (Kc) を有し、これらのデータに対するショップサーバ1010の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ1 (ショップ) には、ショップサーバ1010の公開鍵証明書が添付され、ユーザ機器1020に送付される。なお、ショップサーバ公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ユーザ機器側に送付済みの場合は、必ずしも改めて送付する必要はない。

【0384】(6) 受信データ検証

ショップサーバ1010から暗号化コンテンツ: Kc (content) と、図14 (b) に示す暗号化コンテンツ鍵データ1 (ショップ) を受信したユーザ機器1020は、暗号化コンテンツ鍵データ1 (ショップ) の検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器1020は、まずショップサーバ1010から受領したショップサーバの公開鍵証明書の検証を発行局 (CA) の公開鍵

KpCAを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵KpSHOPを用いて図14 (b) に示す暗号化コンテンツ鍵データ1のショップ署名の検証を実行する。

【0385】(7) 相互認証および属性確認処理

ユーザ機器1020が、ショップサーバ1010から暗号化コンテンツ: Kc (content) と暗号化コンテンツ鍵データ1 (ショップ) を受信し、暗号化コンテンツ鍵データ1 (ショップ) の検証を終えると、ユーザ機器1020は、ユーザ機器認証サーバ1030にアクセスし、ユーザ機器1020と、ユーザ機器認証サーバ1030間において相互認証処理および属性確認処理を実行する。この処理は、前述のショップサーバ1010とユーザ機器1020間の相互認証処理および属性確認処理と同様の手続きで実行される。

【0386】(8) 暗号化コンテンツ鍵データ (ユーザ機器) および暗号化コンテンツ鍵かけかえ要求送信

ユーザ機器1020とユーザ機器認証サーバ1030との間の相互認証および属性確認が成立すると、ユーザ機器1020は、ユーザ機器認証サーバ1030に対して、先にショップサーバ1010から受信した暗号化コンテンツ鍵KpDAS (Kc) と、暗号化コンテンツ鍵かけかえ要求を送信する。暗号化コンテンツ鍵データ (ユーザ機器) の構成は、先に説明した図14 (c) に示す構成である。すなわち、暗号化コンテンツ鍵かけかえ要求の要求先であるユーザ機器認証サーバ1030の識別子であるユーザ機器認証サーバID、ショップサーバ1010から受領した暗号化コンテンツ鍵データ (図14 (b) のショップ公開鍵証明書を除いたデータ)、を有し、これらのデータに対するユーザ機器1020の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ (ユーザ機器) には、ショップサーバ1010の公開鍵証明書と、ユーザ機器1020の公開鍵証明書が添付され、ユーザ機器認証サーバ1030に送付される。なお、ユーザ機器認証サーバ1030がユーザ機器公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【0387】(9) 受信データ検証

ユーザ機器1020から暗号化コンテンツ鍵データ (ユーザ機器) および暗号化コンテンツ鍵かけかえ要求 (図14 (c)) を受信したユーザ機器認証サーバ1030は、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器認証サーバ1030は、まずユーザ機器1020から受領したユーザ機器の公開鍵証明書の検証を発行局 (CA) の公開鍵KpCAを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵KpDEVを用いて図14 (c) に示す暗号化コンテンツ鍵データ (ユーザ機器) の電子署名の

検証を実行する。さらに、ショップサーバの公開鍵証明書の検証を発行局（CA）の公開鍵 K_{pCA} を用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵 K_{pSHOP} を用いて図14（c）に示す暗号化コンテンツ鍵データ（ユーザ機器）に含まれる（5）暗号化コンテンツ鍵データ1のショップ署名の検証を実行する。また、ユーザ機器の送信した電文が図14

（c）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【0388】（10）暗号化コンテンツ鍵かけかえ処理
ユーザ機器認証サーバ1030において、ユーザ機器1020から受信した暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求の検証が終了し、正当な鍵かけかえ要求であると判定すると、ユーザ機器認証サーバ1030は、暗号化コンテンツ鍵データ（ユーザ機器）に含まれる暗号化コンテンツ鍵、すなわち、コンテンツ鍵： K_c をユーザ機器認証サーバ（DAS）1030の公開鍵 K_{pDAS} で暗号化したデータ： $K_{pDAS}(K_c)$ をユーザ機器認証サーバ1030の秘密鍵 K_{sDAS} で復号してコンテンツ鍵 K_c を取得し、さらにコンテンツ鍵 K_c をユーザ機器の公開鍵： K_{pDEV} で暗号化した暗号化コンテンツ鍵： $K_{pDEV}(K_c)$ を生成する。すなわち、 $K_{pDAS}(K_c) \rightarrow K_c \rightarrow K_{pDEV}(K_c)$ の鍵かけかえ処理を実行する。

【0389】この処理は先に図16を用いて説明したように、暗号化コンテンツ鍵データ（ユーザ機器）から、ユーザ機器認証サーバ（DAS）1030の公開鍵 K_{pDAS} で暗号化したコンテンツ鍵データ： $K_{pDAS}(K_c)$ を取り出し、次に、ユーザ機器認証サーバ1030の秘密鍵 K_{sDAS} で復号してコンテンツ鍵 K_c を取得し、次に、復号により取得したコンテンツ鍵 K_c をユーザ機器の公開鍵： K_{pDEV} で再暗号化して暗号化コンテンツ鍵： $K_{pDEV}(K_c)$ を生成する処理である。

【0390】（11）相互認証および属性確認処理
ユーザ機器認証サーバ1030において、上述の暗号化コンテンツ鍵の鍵かけかえ処理が完了すると、ユーザ機器認証サーバ1030は、ショップサーバ1010にアクセスし、ユーザ機器認証サーバ1030とショップサーバ1010間において相互認証処理および属性確認処理を実行する。この処理は、前述のショップサーバ1010とユーザ機器1020間の相互認証処理および属性確認処理と同様の手続きで実行される。

【0391】（12）暗号化コンテンツデータ送信
ユーザ機器認証サーバ1030とショップサーバ1010間の相互認証および属性確認処理が成立すると、ユーザ機器認証サーバ1030は、暗号化コンテンツ鍵データ（DAS）をショップサーバ1010に送信する。暗号化コンテンツ鍵データ（DAS）の構成は、先に説明

した図17（d）に示す構成である。コンテンツ購入の要求先であるショップサーバ1010の識別子であるショップID、暗号化コンテンツ鍵データ（ユーザ機器）

（図14（c）のショップおよびユーザ機器公開鍵証明書を除いたデータ）、さらに、前述の鍵かけかえ処理により、ユーザ機器認証サーバ1030が生成した暗号化コンテンツ鍵データ： $K_{pDEV}(K_c)$ を有し、これらのデータに対するユーザ機器認証サーバ1030の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（DAS）には、ユーザ機器認証サーバ1030と、ユーザ機器1020の公開鍵証明書が添付され、ショップサーバ1010に送付される。なお、ショップサーバが、これらの公開鍵証明書を既に保有済みである場合は、必ずしも改めて送付する必要はない。

【0392】また、ユーザ機器認証サーバ1030が信頼できる第三者機関であると認められる存在である場合は、暗号化コンテンツ鍵データ（DAS）は、図17

（d）に示すようにユーザ機器の生成した（8）暗号化コンテンツ鍵データ（ユーザ機器）をそのまま含むデータ構成とすることなく、図18（d'）に示すように、ユーザ機器ID、トランザクションID、コンテンツID、ショップ処理NO、ユーザデバイスの公開鍵で暗号化したコンテンツ鍵 $K_{pDEV}(K_c)$ の各データを、ユーザ機器認証サーバ1030が抽出して、これらに署名を付加して暗号化コンテンツ鍵データ（DAS）としてもよい。この場合は、（8）暗号化コンテンツ鍵データ（ユーザ機器）の検証が不要となるので、添付する公開鍵証明書は、ユーザ機器認証サーバ1030の公開鍵証明書のみでよい。

【0393】（13）受信データ検証

ユーザ機器認証サーバ1030から暗号化コンテンツ鍵データ（DAS）（図17（d））を受信したショップサーバ1010は、暗号化コンテンツ鍵データ（DAS）の検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ショップサーバ1010は、まずユーザ機器認証サーバ1030から受領したユーザ機器認証サーバの公開鍵証明書の検証を発行局（CA）の公開鍵 K_{pCA} を用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ1030の公開鍵 K_{pDAS} を用いて図17（d）に示す暗号化コンテンツ鍵データ（DAS）の電子署名の検証を実行する。さらに、ユーザ機器の公開鍵証明書の検証を発行局（CA）の公開鍵 K_{pCA} を用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵 K_{pDEV} を用いて図17（d）に示す暗号化コンテンツ鍵データ（DAS）に含まれる（8）暗号化コンテンツ鍵データ（ユーザ機器）のユーザ機器署名の検証を実行する。また、ユーザ機器の送信した電文が図14（c）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【0394】なお、先に説明した図18(d')の簡略化した暗号化コンテンツ鍵データ(DAS)をショップサーバ1010が受領した場合は、ショップサーバ1010は、ユーザ機器認証サーバの公開鍵証明書の検証を発行局(CA)の公開鍵KpCAを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ1030の公開鍵KpDASを用いて図18(d')に示す暗号化コンテンツ鍵データ(DAS)の電子署名の検証を実行するのみの処理となる。

【0395】(14)相互認証および属性確認

(15)暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器1020は、暗号化コンテンツ鍵要求データをショップサーバに対して送信する。なお、この際、前の要求と異なるセッションで要求を実行する場合は、再度相互認証および属性確認を実行して、相互認証および属性確認が成立したことを条件として暗号化コンテンツ鍵要求データがユーザ機器1020からショップサーバ1010に送信される。また、ユーザ機器の送信した電文が図14(c)に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【0396】暗号化コンテンツ鍵要求データの構成は図17(e)に示す通りである。暗号化コンテンツ鍵要求データは、コンテンツ購入の要求先であるショップサーバ1010の識別子であるショップID、取り引きの識別子として、ユーザ機器1020の暗号処理手段が乱数に基づいて生成するトランザクションID、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツID、さらに、先にショップが生成し暗号化コンテンツ鍵データ1(ショップ)としてユーザ機器1020に送信してきたデータ(図14(b)参照)中に含まれるショップ処理No.を有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、暗号化コンテンツ鍵要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ1010に送付される。なお、公開鍵証明書が既にショップ側に保管済みの場合は、必ずしも改めて送付する必要はない。

【0397】(16)検証処理、および

(17)課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ1010は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、図15を用いて説明したと同様の処理である。データ検証が済むと、ショップサーバ1010は、コンテンツの取り引きに関する課金処理を実行する。課金処理は、ユーザの取り引き口座からコンテンツ料金を受領する処理である。受領したコンテンツ料金は、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に配分される。

【0398】この課金処理に至るまでには、ユーザ機器認証サーバ1030による暗号化コンテンツ鍵の鍵かけ

かえ処理プロセスが必須となっているので、ショップサーバ1010は、ユーザ機器間とのみの処理では課金処理が実行できない。また、ユーザ機器1020においても暗号化コンテンツ鍵の復号ができないので、コンテンツの利用ができない。ユーザ機器認証サーバは、図6を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべての課金対象となるコンテンツ取り引きが把握可能となる。従って、ショップ側単独でのコンテンツ取り引きは不可能となり、不正なコンテンツ販売が防止される。

【0399】(18)暗号化コンテンツ鍵データ2(ショップ)送信

ショップサーバ1010における課金処理が終了すると、ショップサーバ1010は、暗号化コンテンツ鍵データ2(ショップ)をユーザ機器1020に送信する。

【0400】暗号化コンテンツ鍵データ2(ショップ)の構成は、先に説明した図17(f)に示す通りである。暗号化コンテンツ鍵要求の要求元であるユーザ機器1020の識別子であるユーザ機器ID、ユーザ機器認証サーバ1030から受領した暗号化コンテンツ鍵データ(DAS)(図17(d)のユーザ機器、ユーザ機器認証サーバ公開鍵証明書を除いたデータ)、を有し、これらのデータに対するショップサーバ1010の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ2(ショップ)には、ショップサーバ1010の公開鍵証明書と、ユーザ機器認証サーバ1030の公開鍵証明書が添付され、ユーザ機器1020に送付される。なお、ユーザ機器1020がユーザ機器認証サーバ公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【0401】なお、ユーザ機器認証サーバ1030が信頼できる第三者機関であると認められる存在であり、ショップサーバ1010がユーザ機器認証サーバ1030から受信する暗号化コンテンツ鍵データ(DAS)が先に説明した図18(d')の簡略化した暗号化コンテンツ鍵データ(DAS)である場合は、ショップサーバ1010は、図18(f')に示す暗号化コンテンツ鍵データ2(ショップ)をユーザ機器に送付する。すなわち、図18(d')に示す簡略化した暗号化コンテンツ鍵データ(DAS)にショップサーバの署名を付加したデータに、ショップサーバ1010の公開鍵証明書と、ユーザ機器認証サーバ1030の公開鍵証明書が添付してユーザ機器1020に送付する。

【0402】(19)受信データ検証

ショップサーバ1010から、暗号化コンテンツ鍵データ2(ショップ)を受領したユーザ機器1020は、暗号化コンテンツ鍵データ2(ショップ)の検証処理を実行する。この検証処理は、先に説明した図15の処理フローと同様の処理であり、ユーザ機器1020は、まず

ショップサーバ1010から受領したショップサーバの公開鍵証明書の検証を発行局(CA)の公開鍵K_pCAを用いて実行し、次に公開鍵証明書から取り出したショップサーバ1010の公開鍵K_pSHOPを用いて図17(f)に示す暗号化コンテンツ鍵データ2(ショップ)の電子署名の検証を実行する。さらに、ユーザ機器認証サーバ1030の公開鍵証明書の検証を発行局(CA)の公開鍵K_pCAを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ1030の公開鍵K_pDASを用いて図17(f)に示す暗号化コンテンツ鍵データ2(ショップ)に含まれる(12)暗号化コンテンツ鍵データ(DAS)の署名検証を実行する。また、何らかの送信電文が図17(f)に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【0403】(20) 保存処理

ショップサーバ1010から受信した暗号化コンテンツ鍵データ2(ショップ)を検証したユーザ機器1020は、暗号化コンテンツ鍵データ2(ショップ)に含まれる自己の公開鍵K_pDEVで暗号化された暗号化コンテンツ鍵:K_pDEV(K_c)を自己の秘密鍵K_sDEVを用いて復号し、さらに、ユーザ機器の保存鍵K_stoを用いて暗号化して暗号化コンテンツ鍵:K_sto(K_c)を生成して、これをユーザ機器1020の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵:K_sto(K_c)を保存鍵K_stoを用いて復号してコンテンツ鍵K_cを取り出して、取り出したコンテンツ鍵K_cを用いて、暗号化コンテンツK_c(Content)の復号処理を実行し、コンテンツ(Content)を再生、実行する。

【0404】以上、述べたように、コンテンツ配信に伴う各処理において、通信を実行する各エンティティは、属性確認により、相手の属性、例えばユーザ機器であることを確認した後、処理を実行する構成としたので、不当なコンテンツ取り引き、例えばショップがユーザ機器になりすましてコンテンツを取り引きするなどの処理、あるいは、ショップサーバになりすまして、ユーザ機器からクレジット口座番号を不正に取得する等の処理が防止される。

【0405】例えばユーザ機器は、属性確認により、ユーザ機器の通信相手がショップであると確認されれば、ショップに対する処理としてのコンテンツ購入に伴う処理を安心して実行可能であり、また属性確認において、通信相手がユーザ機器認証サーバであると確認されれば、ユーザ機器認証サーバに対する処理、例えば鍵のかけかえ要求の送信を実行することができる。本構成によれば、属性確認を行なうことにより通信相手の属性が確認可能となるので、それぞれの通信相手に応じた正当な処理が実行される。さらに、不正な通信相手に秘密データを誤って送信することもなくなるので、データ漏洩の

防止も可能である。

【0406】次に、相互認証処理による相手確認を実行せず、受信データの署名検証のみを実行して、データ改竄の有無と、属性確認を実行してコンテンツ取り引き処理を実行する形態について図74を用いて説明する。

【0407】図74に示す処理は、図72に示す処理から相互認証処理を省いた処理として実行されるものである。図74の番号(1)から(16)の順に処理が進行する。各番号順に処理の詳細を説明する。

【0408】(1) トランザクションID、購入要求データ生成、および

(2) 購入要求データ送信

まず、ユーザ機器1020は、コンテンツの購入要求データを生成し、ショップサーバ1010に送信する。購入要求データの構成は、先に説明した図14(a)に示す構成である。

【0409】(3) 受信データ検証

図14(a)に示す購入要求データをユーザ機器1020から受信したショップサーバは、受信データの検証処理を実行する。本実施例における検証処理は、購入要求データの改竄有無のチェックとともに、属性情報のチェックも併せて実行するものである。

【0410】図75に公開鍵証明書に属性情報が格納されている場合の受信データ検証処理フローを示す。まず、メッセージと署名(購入要求データ)と、ユーザ機器の公開鍵証明書を受信(S2301)したショップサーバ1010は、ユーザ機器の公開鍵証明書を公開鍵証明書発行局の公開鍵K_pCAを用いて検証(S2302)する。検証が成立(S2303でYes)すると、公開鍵証明書からユーザ機器の公開鍵:K_pDEVを取り出し(S2304)て、ユーザ機器の公開鍵:K_pDEVを用いて購入要求データのユーザ機器署名の検証(S2305)を行なう。さらに、検証が成功(S2306でYes)すると、公開鍵証明書から属性情報を取り出し(S2307)て、正当な属性(ここではユーザ機器を示す属性)であるか否かを判定(S2308)し、正当である場合は、検証処理成功(S2309)として、次の処理に移行する。ステップS2303、S2306、S2308で判定がNoの場合は、検証処理失敗(S2310)として処理を中止する。

【0411】次に、公開鍵証明書と属性証明書を用いた受信データ検証処理について図76のフローを用いて説明する。まず、メッセージと署名(購入要求データ)と、ユーザ機器の公開鍵証明書、属性証明書を受信(S2401)したショップサーバ1010は、ユーザ機器の公開鍵証明書を公開鍵証明書発行局の公開鍵K_pCAを用いて検証(S2402)する。検証が成立(S2403でYes)すると、公開鍵証明書からユーザ機器の公開鍵:K_pDEVを取り出し(S2404)て、ユーザ機器の公開鍵:K_pDEVを用いて購入要求データの

ユーザ機器署名の検証(S2405)を行なう。さらに、検証が成功(S2406でYes)すると、属性証明書を属性証明書発行局の公開鍵KpAAを用いて検証(S2407)する。検証が成功(S2408でYes)したことを条件として、属性証明書から属性情報を取り出し(S2409)て、正当な属性(ここではユーザ機器を示す属性)であるか否かを判定(S2410)し、正当である場合は、検証処理成功(S2411)として、次の処理に移行する。ステップS2403、S2406、S2408、S2410で判定がNoの場合は、検証処理失敗(S2412)として処理を中止する。

【0412】(4) 暗号化コンテンツおよび暗号化コンテンツ鍵データ1(ショップ)送信

ショップサーバ1010において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定され属性が確認されると、ショップサーバ1010は、暗号化コンテンツおよび暗号化コンテンツ鍵データ1(ショップ)(図14(b)参照)をユーザ機器に送信する。

【0413】(5) 受信データ検証

ショップサーバ1010から暗号化コンテンツ:Kc(content)と、図14(b)に示す暗号化コンテンツ鍵データ1(ショップ)を受信したユーザ機器1020は、暗号化コンテンツ鍵データ1(ショップ)の検証処理および属性確認処理を実行する。この検証処理は、先に説明した図75または図76の処理フローと同様の処理である。この場合、公開鍵証明書または属性証明書の属性がショップを示していない場合は、処理が中止されることになる。

【0414】(6) 暗号化コンテンツ鍵データ(ユーザ機器)および暗号化コンテンツ鍵かけかえ要求送信

次に、ユーザ機器1020は、ユーザ機器認証サーバ1030に対して、先にショップサーバ1010から受信した暗号化コンテンツ鍵KpDAS(Kc)と、暗号化コンテンツ鍵かけかえ要求(図14(c)参照)を送信する。

【0415】(7) 受信データ検証

ユーザ機器1020から暗号化コンテンツ鍵データ(ユーザ機器)および暗号化コンテンツ鍵かけかえ要求(図14(c))を受信したユーザ機器認証サーバ1030は、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。この検証処理は、先に説明した図75、図76の処理フローと同様の処理であり、属性確認も併せて実行する処理である。この場合は公開鍵証明書または属性証明書の属性がユーザ機器でない場合は、処理が中止される。

【0416】(8) 暗号化コンテンツ鍵かけかえ処理、次に、ユーザ機器認証サーバ1030において、KpDAS(Kc)→Kc→KpDEV(Kc)の鍵かけかえ

処理を実行する。

【0417】(9) 暗号化コンテンツデータ送信

次に、ユーザ機器認証サーバ1030は、暗号化コンテンツ鍵データ(DAS)をショップサーバ1010に送信する。暗号化コンテンツ鍵データ(DAS)の構成は、先に説明した図17(d)に示す構成である。

【0418】(10) 受信データ検証

ユーザ機器認証サーバ1030から暗号化コンテンツ鍵データ(DAS)(図17(d))を受信したショップサーバ1010は、暗号化コンテンツ鍵データ(DAS)の検証処理を実行する。この検証処理は、先に説明した図75、図76の処理フローと同様の処理であり、属性確認が併せて実行される。この場合は公開鍵証明書または属性証明書の属性がユーザ機器認証サーバ(サービス運営体)でない場合は、処理が中止される。

【0419】(11) 暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器1020は、暗号化コンテンツ鍵要求データをショップサーバに対して送信する。暗号化コンテンツ鍵要求データの構成は図17(e)に示す通りである。

【0420】(12) 検証処理、および

(13) 課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ1010は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、先に説明した図75、図76の処理フローと同様の処理であり、属性確認も併せて実行する処理である。この場合は公開鍵証明書または属性証明書の属性がユーザ機器でない場合は、処理が中止される。データ検証が済むと、ショップサーバ1010は、コンテンツの取り引きに関する課金処理を実行する。

【0421】(14) 暗号化コンテンツ鍵データ2(ショップ)送信

ショップサーバ1010における課金処理が終了すると、ショップサーバ1010は、暗号化コンテンツ鍵データ2(ショップ)をユーザ機器1020に送信する。暗号化コンテンツ鍵データ2(ショップ)の構成は、先に説明した図17(f)に示す通りである。

【0422】(15) 受信データ検証

(16) 保存処理

ショップサーバ1010から、暗号化コンテンツ鍵データ2(ショップ)を受領したユーザ機器1020は、暗号化コンテンツ鍵データ2(ショップ)の検証処理を実行する。この検証処理は、先に説明した図75、図76の処理フローと同様の処理であり、属性確認も併せて実行する処理である。この場合は公開鍵証明書または属性証明書の属性がショップでない場合は、処理が中止される。データ検証が済むと、ユーザ機器1020は、コンテンツの保存処理、すなわち自己の公開鍵KpDEVで

暗号化された暗号化コンテンツ鍵：K_{pDEV}（K_c）を自己の秘密鍵K_{sDEV}を用いて復号し、さらに、ユーザ機器の保存鍵K_{sto}を用いて暗号化して暗号化コンテンツ鍵：K_{sto}（K_c）を生成して、これをユーザ機器1020の記憶手段に格納する処理を実行する。

【0423】このように、図74に示す処理においては、相互認証時に属性確認を行なうのではなく、受信したデータの署名検証において、属性を確認する処理を実行する構成としたので、処理が簡略化され、コンテンツ取り引きに伴う処理の効率化が達成される。

【0424】なお、上述した属性データによる属性確認を適用した実施例では、サービス運営体において、鍵かけかえ処理を実行する構成について説明したが、例えば前述のログ収集サーバを適用した構成においても属性確認処理を適用することが可能である。その他一般的なデータ送受信を実行するエンティティ間において、それぞれのエンティティに特徴づけられた機能に基づいて属性を設定し、設定された属性を公開鍵証明書または属性証明書に格納し、これらの証明書を用いて通信相手の属性確認処理を実行することにより、さらにデータ通信の安全性、セキュリティを高めることが可能となる。また、属性確認処理は、従来の相互認証処理、署名検証処理と併せて実行することが可能であるので、通常データ通信は、署名検証のみ、あるいは相互認証のみを行ない、必要に応じて属性確認処理を行なうなど、セキュリティ度合いに応じて選択的に署名検証処理、相互認証処理、属性確認処理のいずれか、あるいは組み合わせて実行することが可能である。

【0425】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0426】

【発明の効果】上述したように、本発明の属性確認処理を含むデータ通信システムおよび属性確認処理を含むデータ通信方法によれば、データ通信を実行するエンティティ間において、通信相手のエンティティに設定された属性情報を通信相手のエンティティの公開鍵証明書または属性証明書から取得し、取得した属性情報に基づく属性確認がなされたことを処理実行条件としたので、通信相手が他のエンティティになりすまして処理を実行することが防止され、安全なデータ通信、例えばコンテンツ取り引きに伴う処理が可能となる。

【0427】さらに、本発明の属性確認処理を含むデータ通信システムおよび属性確認処理を含むデータ通信方法によれば、例えば、コンテンツの購入を実行するユーザ機器、コンテンツの購入要求を受け付けるショップサ

ーバ、コンテンツ配信管理を行うシステムホルダ等の機能毎に異なる属性コードを付与して、属性コードに基づいて属性確認を実行する構成としたので、ユーザ機器は例えば通信相手がショップサーバであることを確認した後、様々なコンテンツ購入処理に伴うデータ送信が可能となり、秘密データの漏洩等が防止される。

【0428】さらに、本発明の属性確認処理を含むデータ通信システムおよび属性確認処理を含むデータ通信方法によれば、属性情報は、公開鍵証明書または属性証明書に格納され、それぞれの証明書には、公開鍵証明書発行局または属性証明書発行局の署名が生成されて格納された構成であるので、不正な属性情報を用いた不正な処理が防止可能となる。

【図面の簡単な説明】

【図1】本発明のコンテンツ配信システムのシステム概要およびコンテンツ配信処理を説明する図である。

【図2】本発明のコンテンツ配信システムにおけるショップサーバの構成を示す図である。

【図3】本発明のコンテンツ配信システムにおけるショップサーバの購買管理データベースの構成を示す図である。

【図4】本発明のコンテンツ配信システムにおけるショップサーバの制御手段構成を示す図である。

【図5】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバの構成を示す図である。

【図6】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバのライセンス管理データベースの構成を示す図である。

【図7】本発明のコンテンツ配信システムにおけるユーザ機器の構成を示す図である。

【図8】本発明のコンテンツ配信システムにおけるユーザ機器の購入管理データベース構成を示す図である。

【図9】本発明のコンテンツ配信システムにおける公開鍵証明書配布構成を示す図である。

【図10】本発明のコンテンツ配信システムにおいて適用可能な署名生成処理を説明する図である。

【図11】本発明のコンテンツ配信システムにおいて適用可能な署名検証処理を説明する図である。

【図12】本発明のコンテンツ配信システムにおいて適用可能な相互認証（対称鍵方式）処理を説明する図である。

【図13】本発明のコンテンツ配信システムにおいて適用可能な相互認証（非対称鍵方式）処理を説明する図である。

【図14】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。

【図15】本発明のコンテンツ配信システムにおいて適用可能なデータ検証処理を説明する図である。

【図16】本発明のコンテンツ配信システムにおいて実

行される鍵かけかえ処理を説明する図である。

【図17】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。

【図18】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。

【図19】本発明のコンテンツ配信システムにおいて実行されるコンテンツ鍵保存処理を説明する図である。

【図20】本発明のコンテンツ配信システムにおけるショップサーバのステータス変遷を説明する図である。

【図21】本発明のコンテンツ配信システムにおけるユーザ機器のステータス変遷を説明する図である。

【図22】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバのステータス変遷を説明する図である。

【図23】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その1）を示す図である。

【図24】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その2）を示す図である。

【図25】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバとユーザ機器間の処理フローを示す図である。

【図26】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバとショップサーバ間の処理フローを示す図である。

【図27】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その1）を示す図である。

【図28】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その2）を示す図である。

【図29】本発明のコンテンツ配信システムの変形例として配信サーバを用いたコンテンツ配信処理を説明する図である。

【図30】本発明のコンテンツ配信システムの変形例として配信サーバを用いたコンテンツ配信処理を説明する図である。

【図31】本発明のコンテンツ配信システムの変形例のコンテンツ配信処理を説明する図である。

【図32】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。

【図33】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。

【図34】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図で

ある。

【図35】本発明のコンテンツ配信システムの相互認証を伴わないコンテンツ配信処理を説明する図である。

【図36】本発明のコンテンツ配信システムの相互認証を伴わないコンテンツ配信処理の変形例を説明する図である。

【図37】本発明のコンテンツ配信システムにおいて電子チケットを適用したコンテンツ配信処理を説明する図である。

【図38】本発明のコンテンツ配信システムのチケット発行サーバの構成を説明する図である。

【図39】本発明のコンテンツ配信システムのチケット発行サーバのチケット発行管理データベース構成を説明する図である。

【図40】本発明のコンテンツ配信システムのユーザ機器の購入管理データベース構成を説明する図である。

【図41】本発明のコンテンツ配信システムのユーザ機器認証サーバのライセンス管理データベース構成を説明する図である。

【図42】本発明のコンテンツ配信システムの配信サーバの構成を説明する図である。

【図43】本発明のコンテンツ配信システムの配信サーバの配信管理データベース構成を説明する図である。

【図44】本発明のコンテンツ配信システムのチケット換金サーバの構成を説明する図である。

【図45】本発明のコンテンツ配信システムのチケット換金サーバのチケット換金管理データベース構成を説明する図である。

【図46】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。

【図47】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。

【図48】本発明のコンテンツ配信システムにおけるチケット発行サーバのステータス変遷を説明する図である。

【図49】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバのステータス変遷を説明する図である。

【図50】本発明のコンテンツ配信システムにおける配信サーバのステータス変遷を説明する図である。

【図51】本発明のコンテンツ配信システムにおけるユーザ機器のステータス変遷を説明する図である。

【図52】本発明のコンテンツ配信システムにおけるチケット換金サーバのステータス変遷を説明する図である。

【図53】本発明のコンテンツ配信システムにおいて電子チケットを適用したコンテンツ配信処理の具体例を説明する図である。

【図54】本発明のコンテンツ配信システムにおいてログ収集サーバを適用したコンテンツ配信処理を説明する図である。

【図55】本発明のコンテンツ配信システムにおける購入ログの構成例を説明する図である。

【図56】本発明のコンテンツ配信システムにおけるログ収集サーバの構成を示す図である。

【図57】本発明のコンテンツ配信システムにおけるユーザ機器と、ショップサーバ間の処理を示すフロー図（その1）である。

【図58】本発明のコンテンツ配信システムにおけるユーザ機器と、ショップサーバ間の処理を示すフロー図（その2）である。

【図59】本発明のコンテンツ配信システムにおける購入要求データと販売確認データのフォーマット例を示す図である。

【図60】本発明のコンテンツ配信システムにおいて着ようか可能な改竄チェック値（ICV）生成処理構成を示す図である。

【図61】本発明のコンテンツ配信システムにおけるユーザ機器と、ログ収集サーバ間の処理を示すフロー図（その1）である。

【図62】本発明のコンテンツ配信システムにおけるユーザ機器と、ログ収集サーバ間の処理を示すフロー図（その2）である。

【図63】本発明のコンテンツ配信システムにおけるコンテンツプロバイダと、ログ収集サーバ間の処理を示すフロー図である。

【図64】本発明のコンテンツ配信システムにおけるショップサーバと、ログ収集サーバ間の処理を示すフロー図である。

【図65】本発明のコンテンツ配信システムにおけるショップサーバと、ログ収集サーバ間の処理を示すフロー図である。

【図66】本発明のコンテンツ配信システムにおいて適用される属性情報について説明する図である。

【図67】本発明のコンテンツ配信システムにおいて適用可能な属性情報を持つ公開鍵証明書構成を示す図である。

【図68】本発明のコンテンツ配信システムにおいて適用可能な公開鍵証明書および属性証明書構成を示す図である。

【図69】本発明のコンテンツ配信システムにおける公開鍵証明書の新規発行処理を説明する図である。

【図70】本発明のコンテンツ配信システムにおける公開鍵証明書の更新処理を説明する図である。

【図71】本発明のコンテンツ配信システムにおける属性証明書の新規発行処理を説明する図である。

【図72】本発明のコンテンツ配信システムにおける属性チェックを伴うコンテンツ配信処理を説明する図であ

る。

【図73】本発明のコンテンツ配信システムにおける属性チェックを伴う相互認証処理を説明するフロー図である。

【図74】本発明のコンテンツ配信システムにおける属性チェックを伴うコンテンツ配信処理を説明する図である。

【図75】本発明のコンテンツ配信システムにおける属性チェックを伴うデータ検証処理を説明するフロー図である。

【図76】本発明のコンテンツ配信システムにおける属性チェックを伴うデータ検証処理を説明するフロー図である。

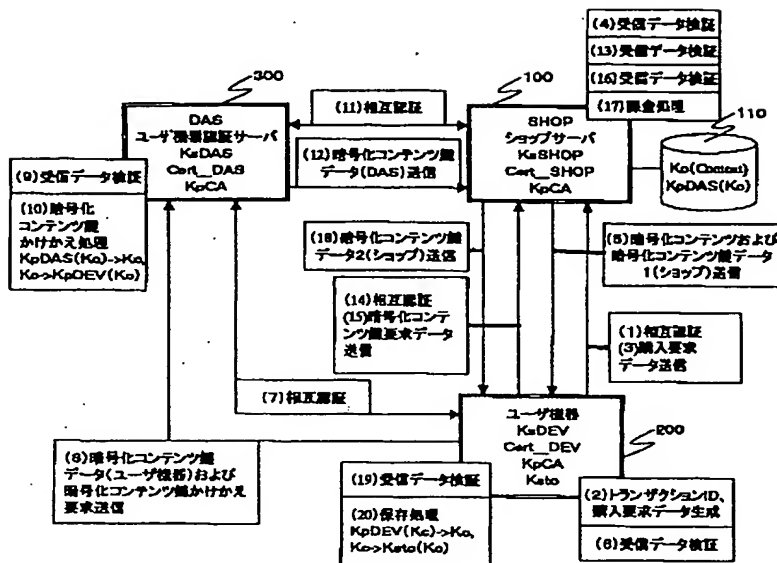
【符号の説明】

100	ショップサーバ
110	コンテンツデータベース
120	購買管理データベース
130	制御手段
131	制御部
132	ROM
133	RAM
134	表示部
135	入力部
136	HDD
137	ドライブ
138	ネットワークインタフェース
200	ユーザ機器
220	購入管理データベース
230	制御手段
300	ユーザ機器認証サーバ
320	ライセンス管理データベース
330	制御手段
400	配信サーバ
410	コンテンツデータベース
610	チケット発行サーバ
612	購買管理データベース
613	制御手段
620	ユーザ機器
630	ユーザ機器認証サーバ
640	配信サーバ
642	配信管理データベース
643	制御手段
644	コンテンツデータベース
650	チケット換金サーバ
652	チケット換金管理データベース
653	制御手段
801	チケット発行体
802	ユーザ機器
803	ライセンスホルダ
804	コンテンツ制作者

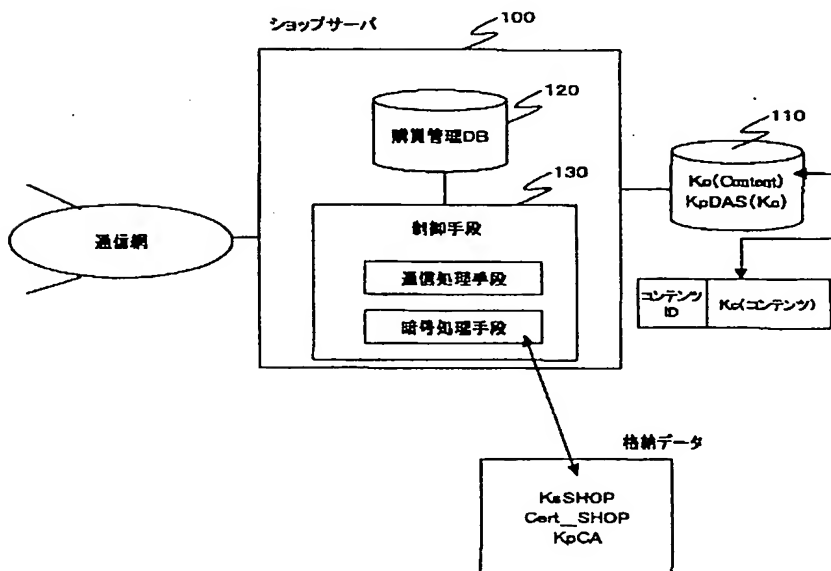
805 銀行
 901 ショップサーバ
 902 ユーザ機器
 903 ログ収集サーバ
 904 オーサリングサーバ
 905 コンテンツプロバイダ
 9031 ログ管理データベース

9032 制御手段
 1010 ショップサーバ
 1020 ユーザ機器
 1030 サービス運営体
 1040 公開鍵証明書発行局
 1050 属性証明書発行局

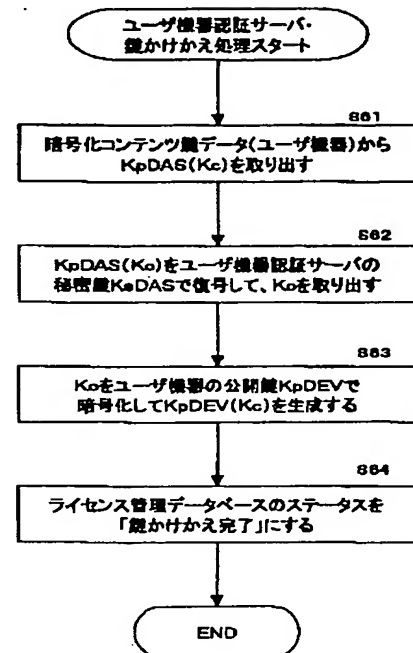
【図1】



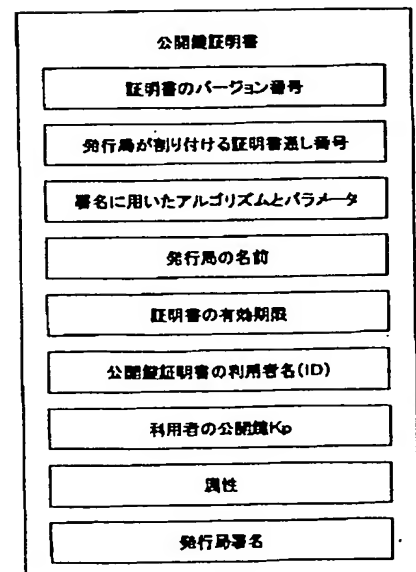
【図2】



【図16】



【図67】

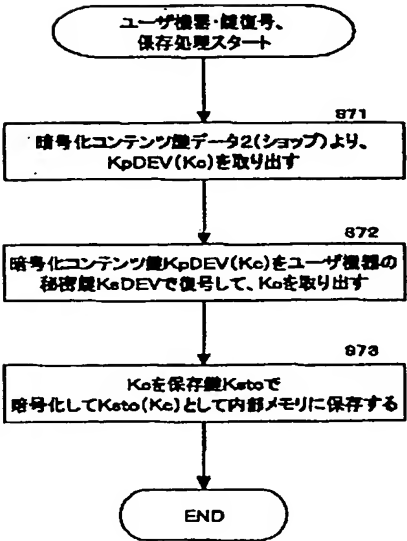


【図3】

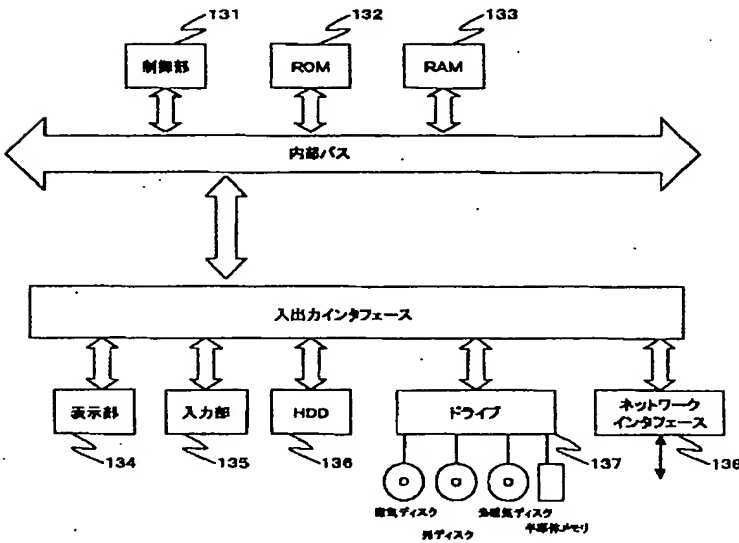
ショップ処理No.	機器ID	トランザクションID	コンテンツID	ステータス
10001	1234567890	999888777	5000	機2配信完了
10002	2345678901	666555444	4050	課金完了
10003	3456789012	333222111	1000	暗号化コンテンツ鍵 送信要求受付完了
10004	4567890123	000999888	3000	機受信完了
10005	5678901234	777666555	5050	機1配信完了
10006	6789012345	444333222	2050	購入受付完了

ショップサーバ・購買管理DB

【図19】



【図4】

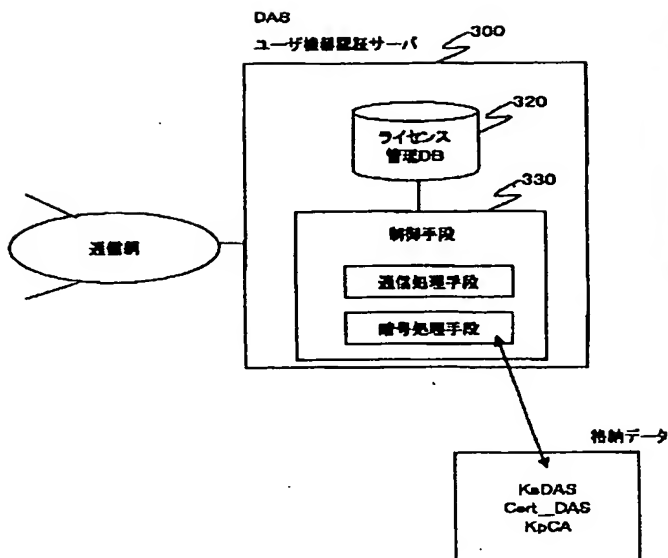


【図6】

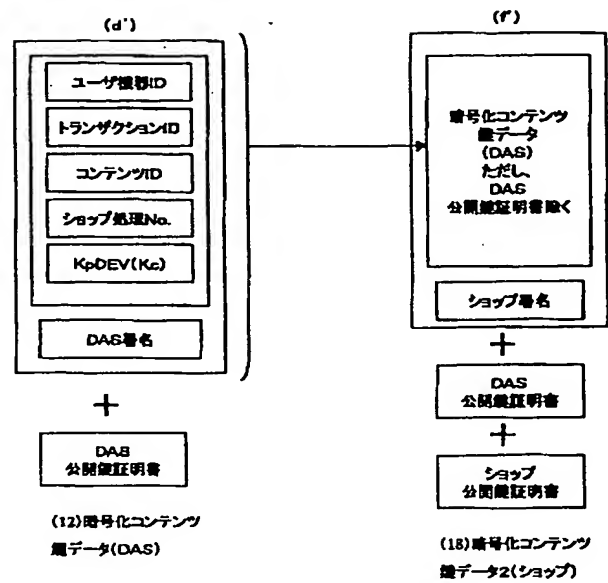
ユーザ機器認証 サーバ処理No.	機器ID	トランザクションID	コンテンツID	ショップID	ショップ処理No.	ステータス
50001	1234567890	999888777	5000	1234	10001	機送信完了
50002	2345678901	666555444	4050	1234	10002	機かけかえ完了

ユーザ機器認証サーバ・ライセンス管理DB

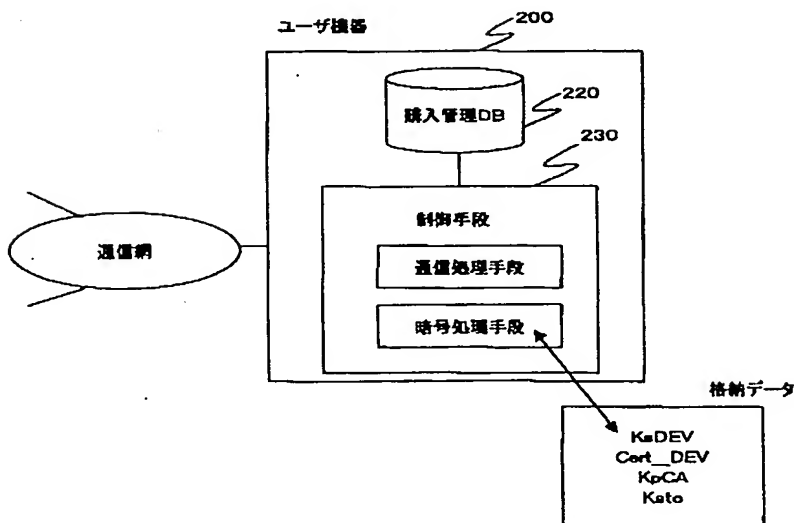
【図5】



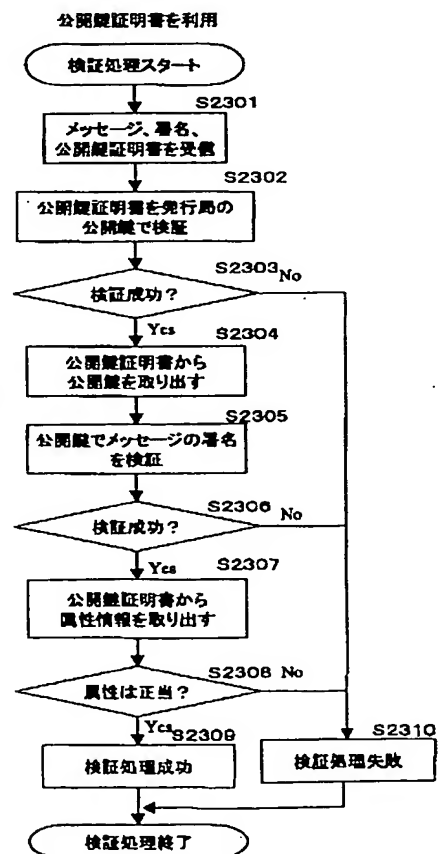
【図18】



【図7】



【図75】



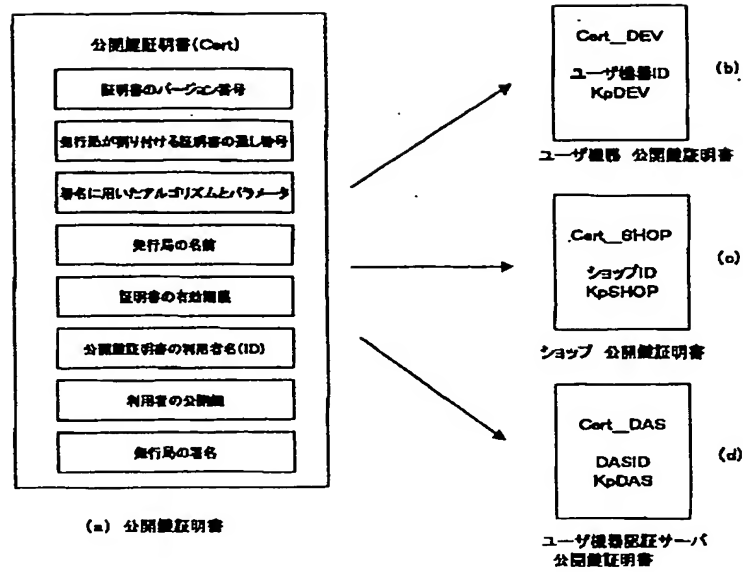
【図8】

機器ID: 1234567890

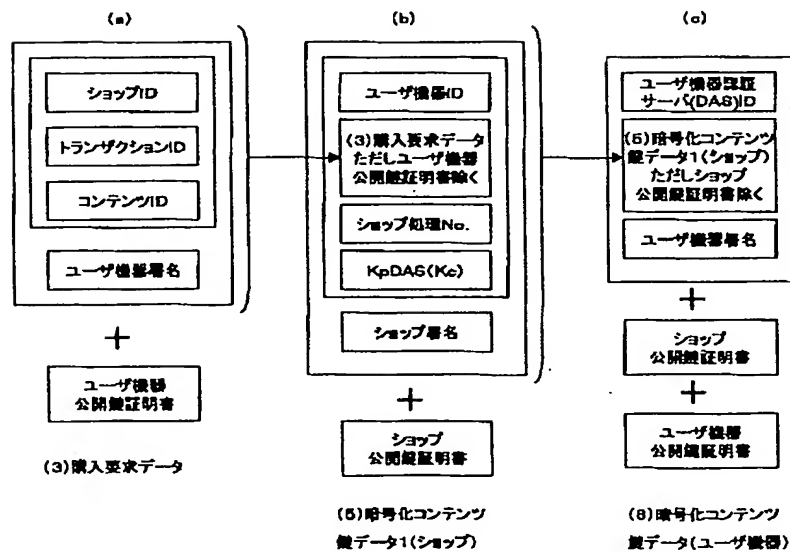
トランザクションID	コンテンツID	ショップID	ステータス
999888777	5000	1234	第2受信完了
666555444	4050	9876	購入要求送信完了

ユーザ機器・購入管理DB

【図9】

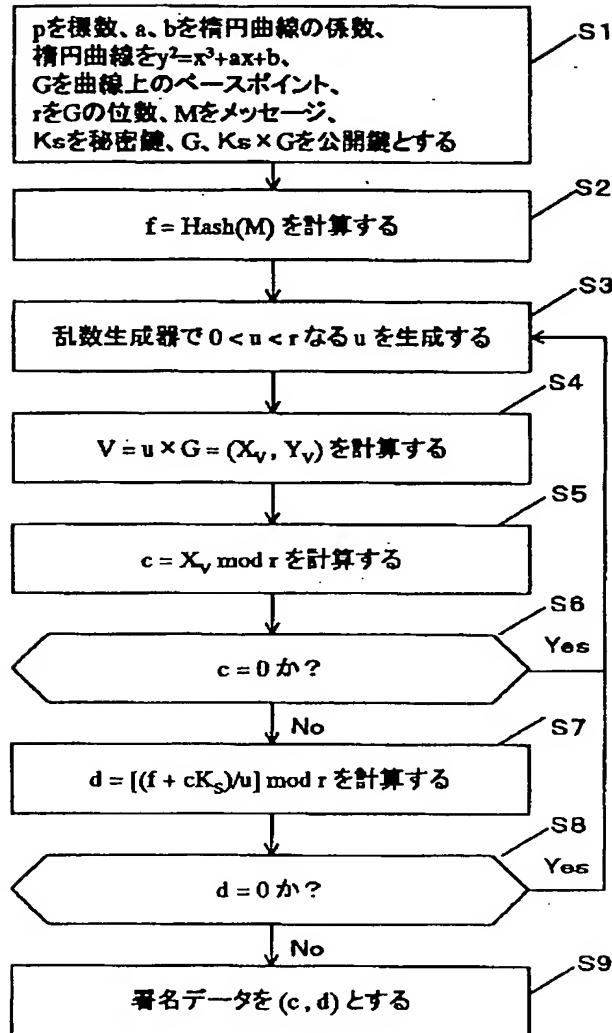


【図14】

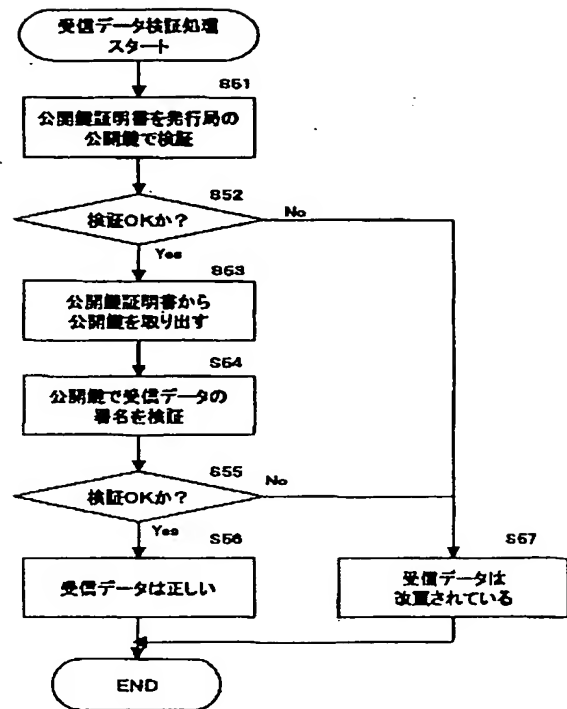


【図10】

署名生成



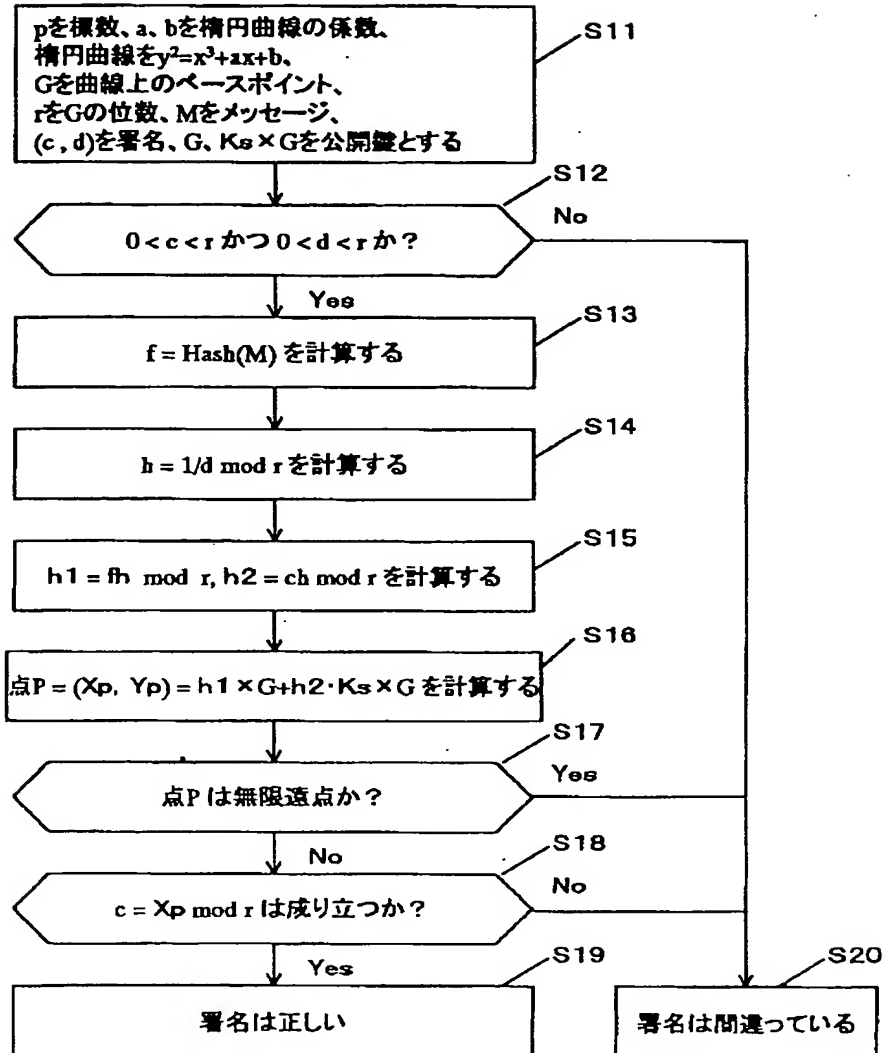
【図15】



署名生成(IEEE P1363/D13)

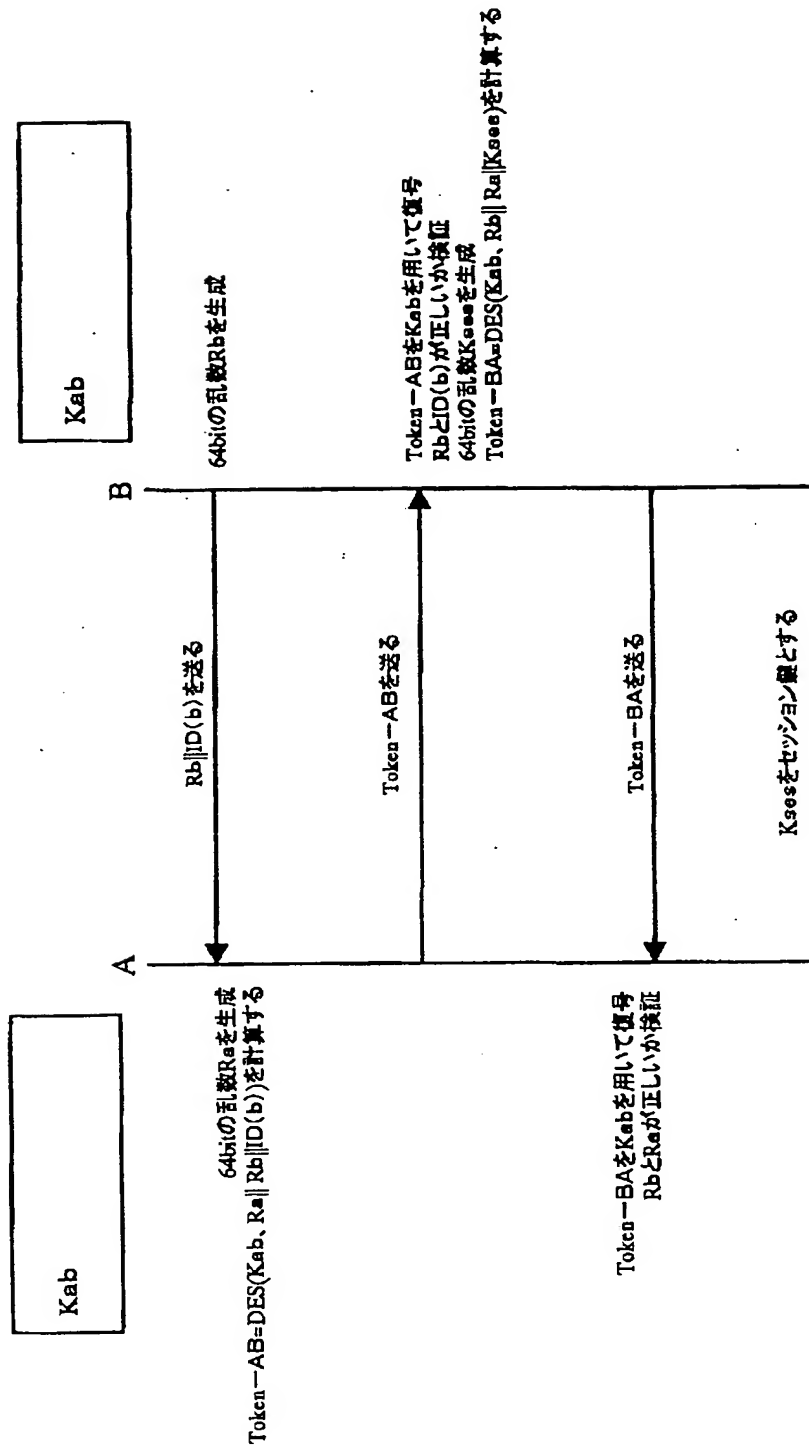
【図11】

署名検証



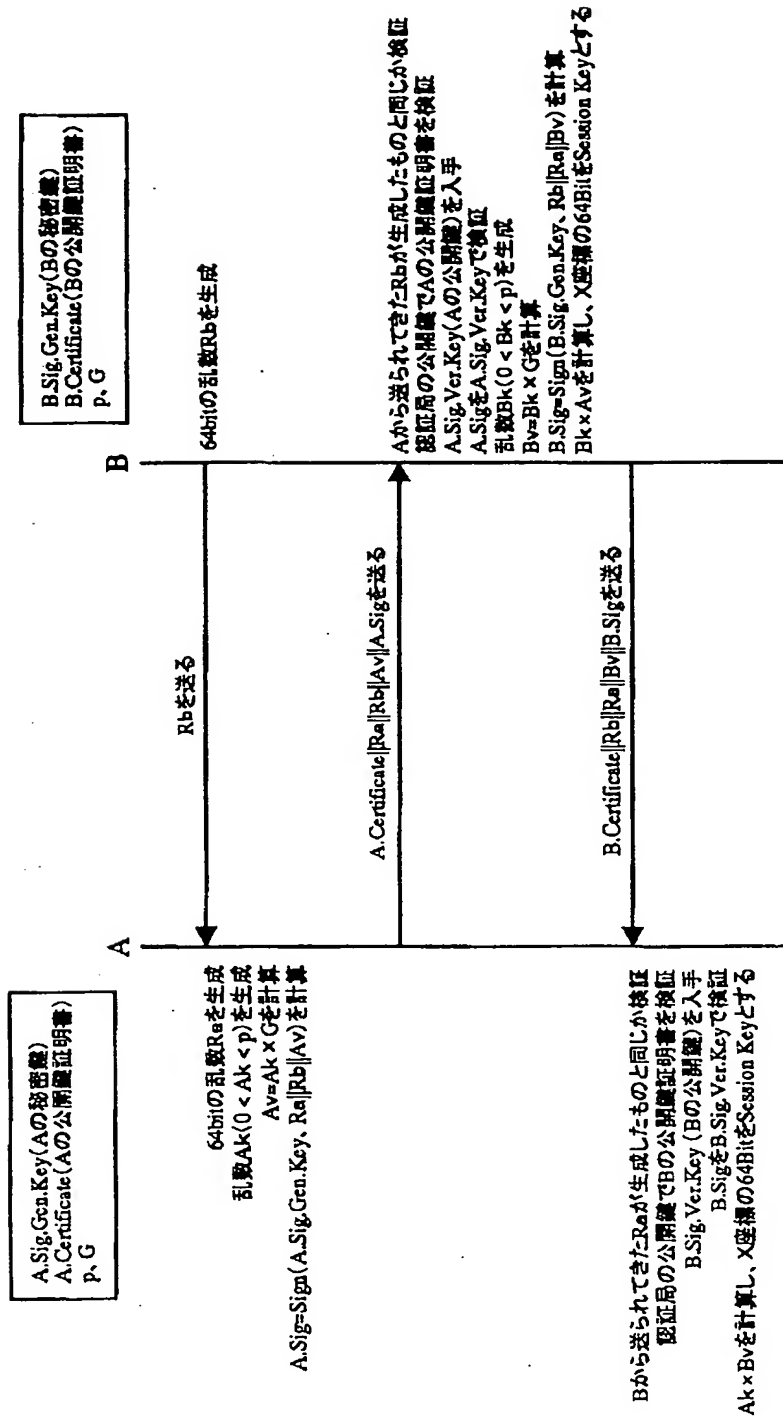
署名検証(IEEE P1363/D13)

【図12】



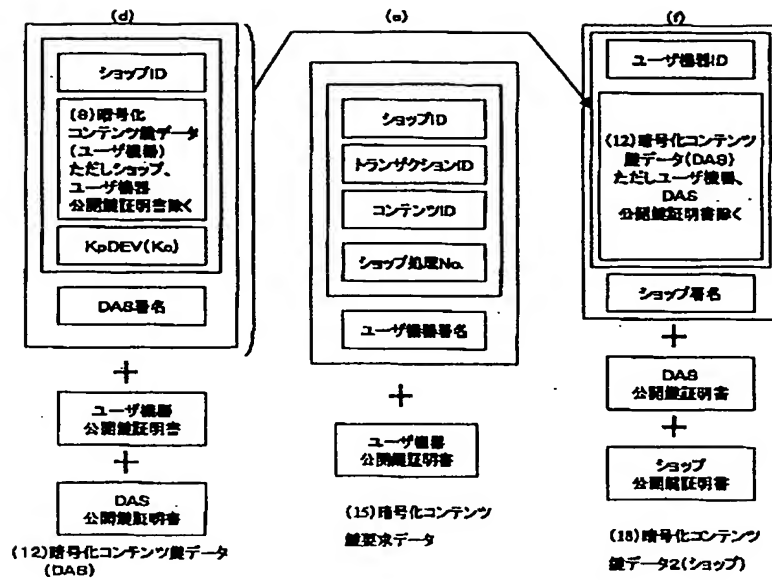
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図13】

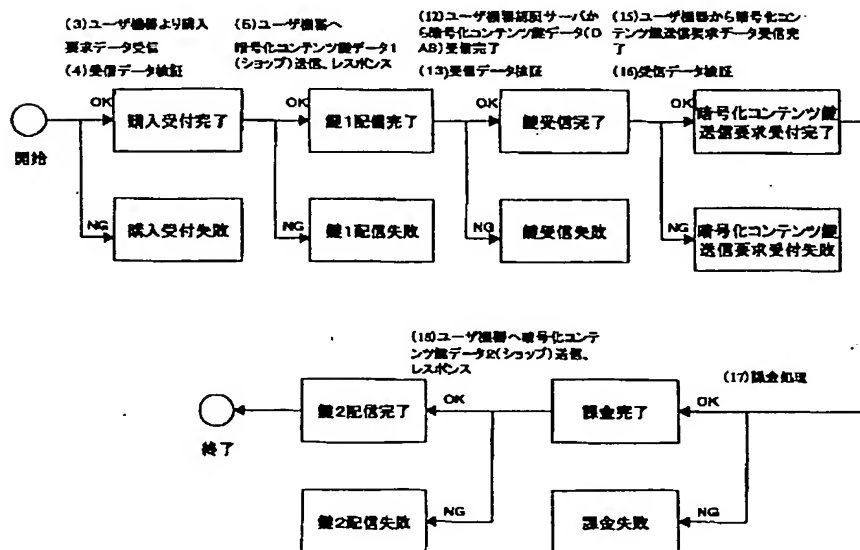


ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

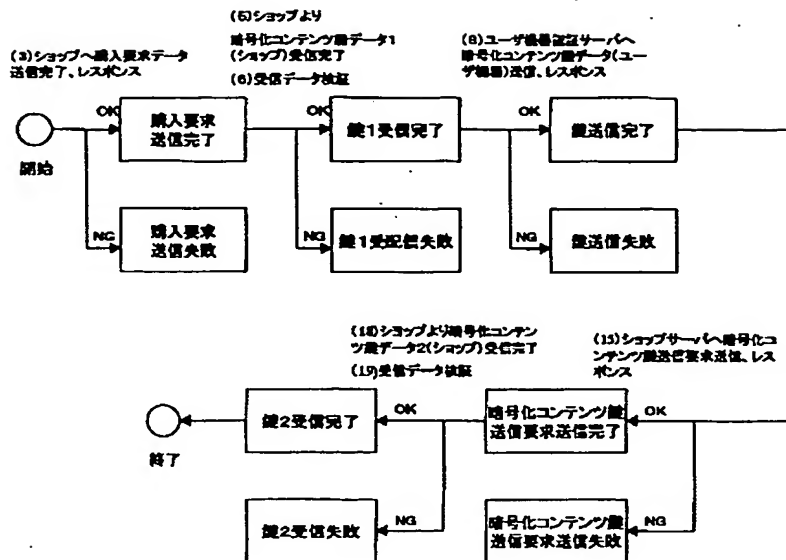
【図17】



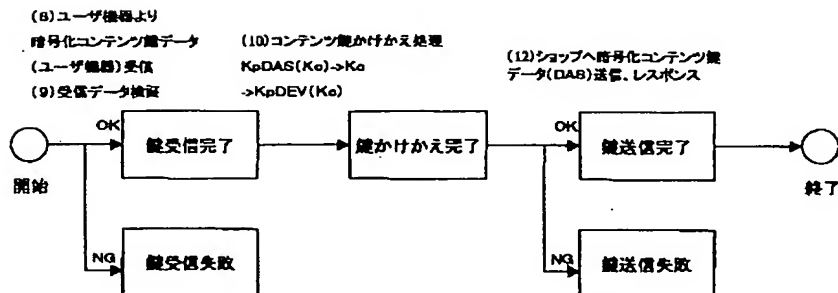
【図20】



【図21】



【図22】

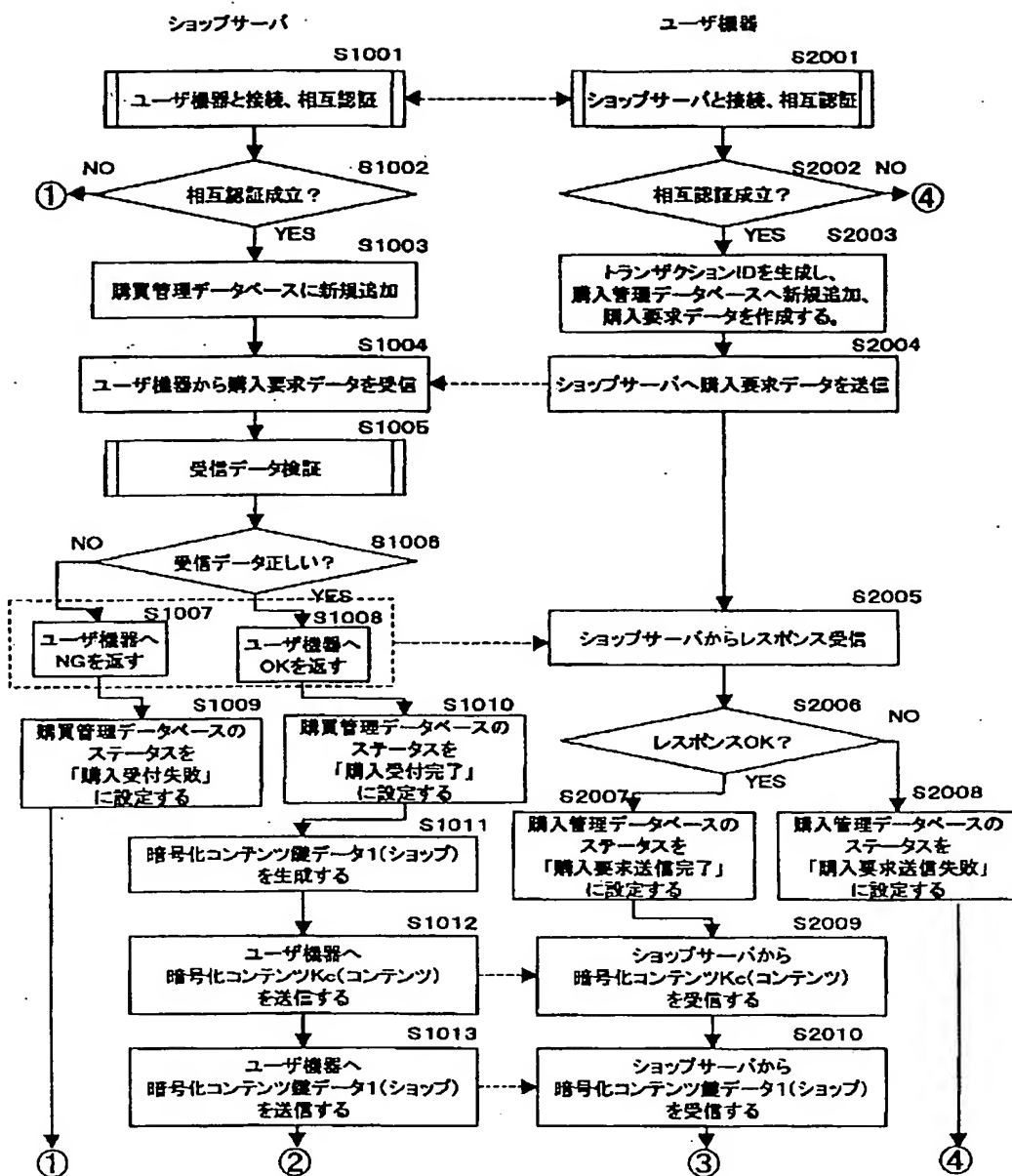


【図39】

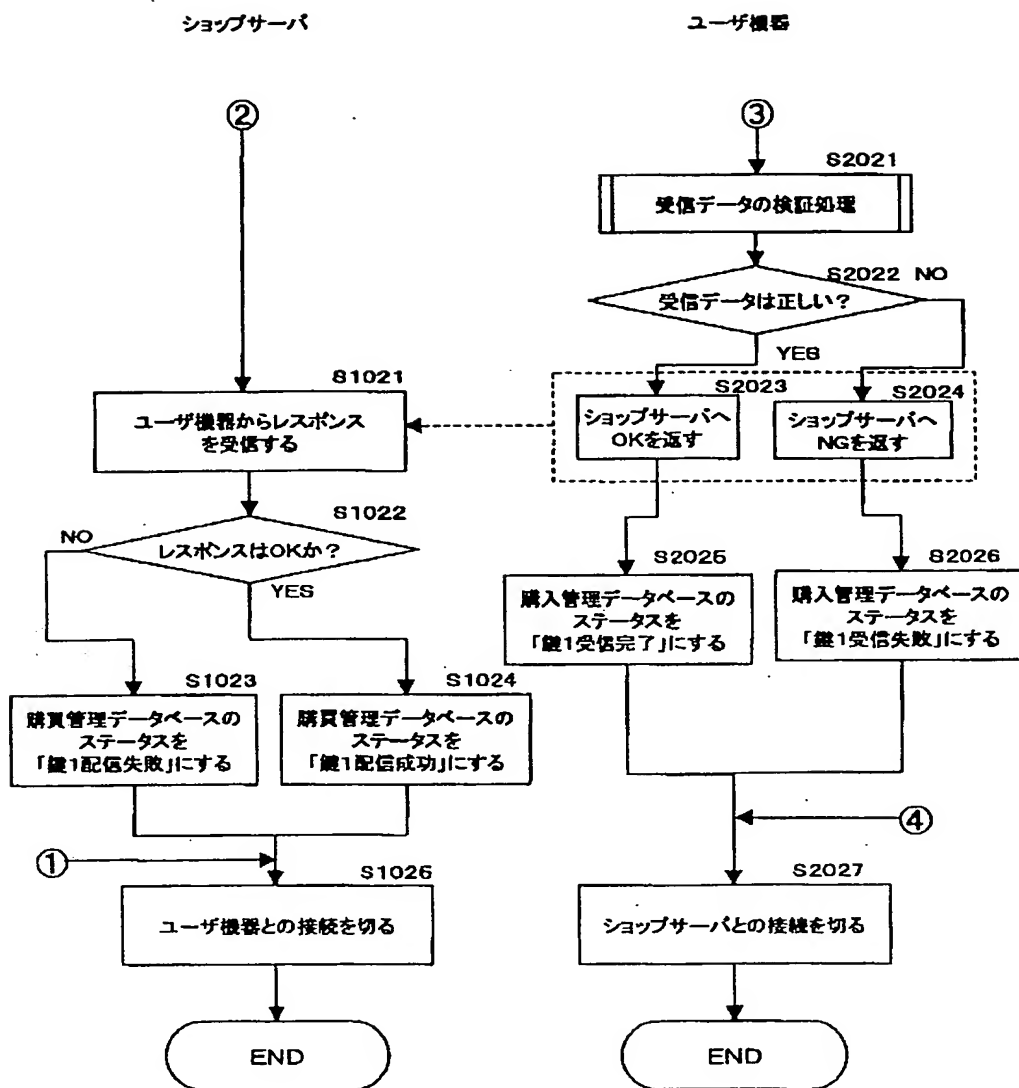
チケット発行 処理No.	機器ID	トランザクションID	コンテンツID	チケット利用先 ID	金額	有効期限	ステータス
10001	1234567890	999888777	5000	222331234	¥1000	00/04/01	換金処理 レポート受信完了
10002	2345678901	666555444	4050	223345634	¥250	00/07/31	電子チケット 配信完了
10003	3456788901	321655444	4021	345645234	¥800	00/07/31	購入受付完了

チケット発行サーバ・チケット発行管理DB

【図23】



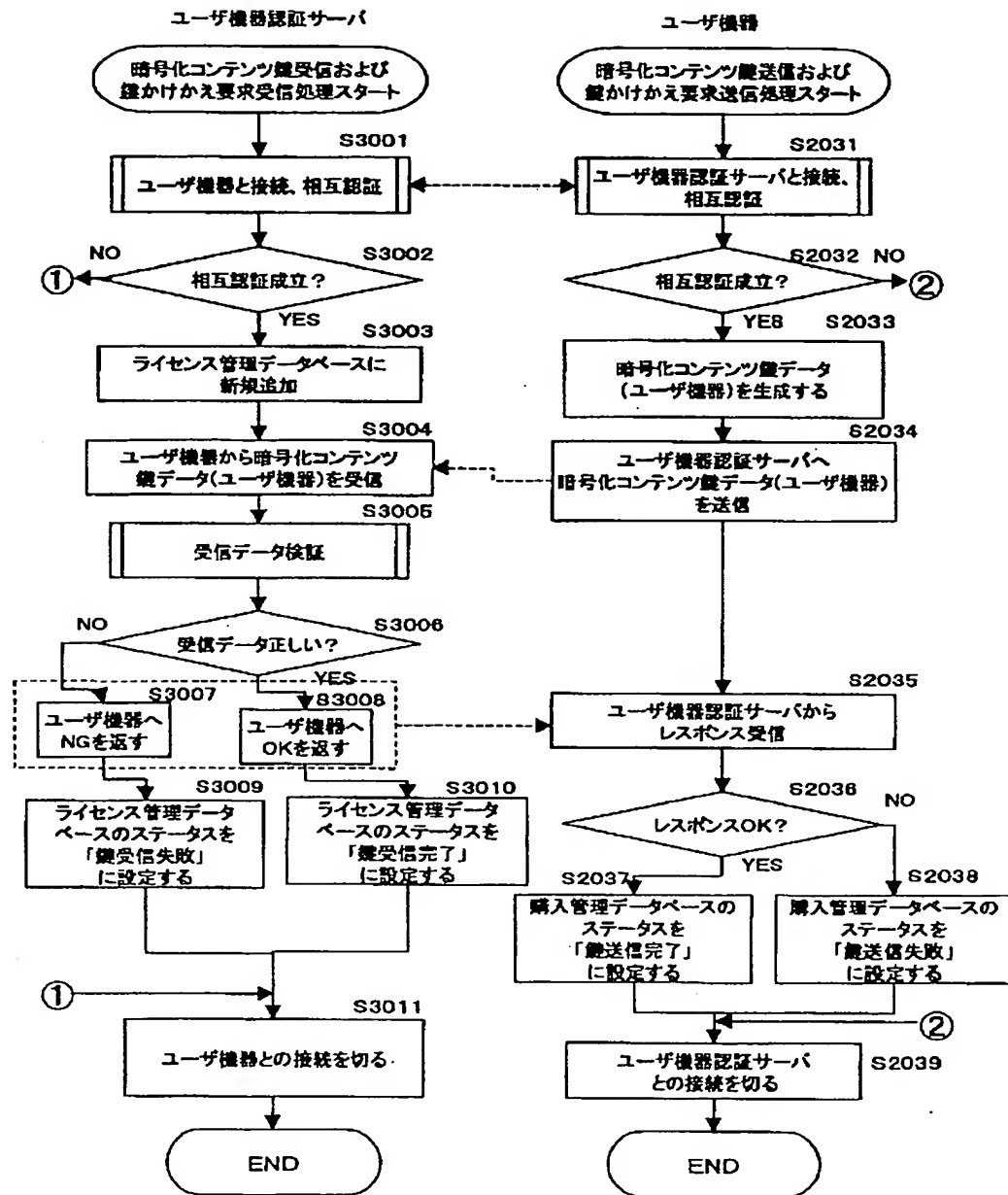
【図24】



【図40】

トランザクションID	コンテンツID	チケット発行体ID	チケット発行処理No.	チケット配信先ID	ステータス
999888777	5000	1234	10001	1234567890	鍵2受信完了
666555444	4050	1534	12345	2345678901	鍵1受信完了
999888779	5010	2351	15435	2233567890	電子チケット送信完了
333555444	4320	0989	10302	—	電子チケット受信完了
2133545445	3232	3549	22543	—	購入要求送信完了

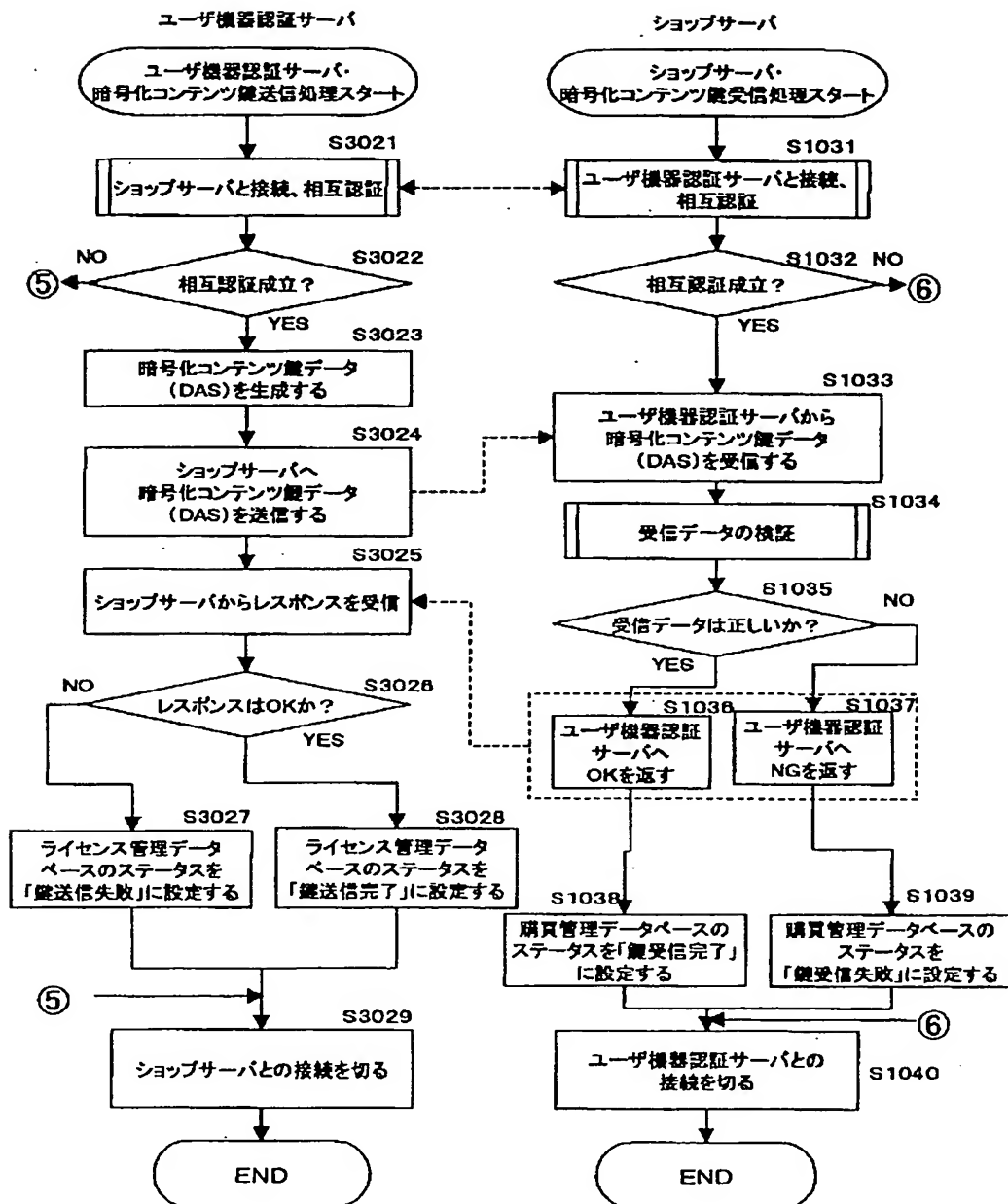
【図25】



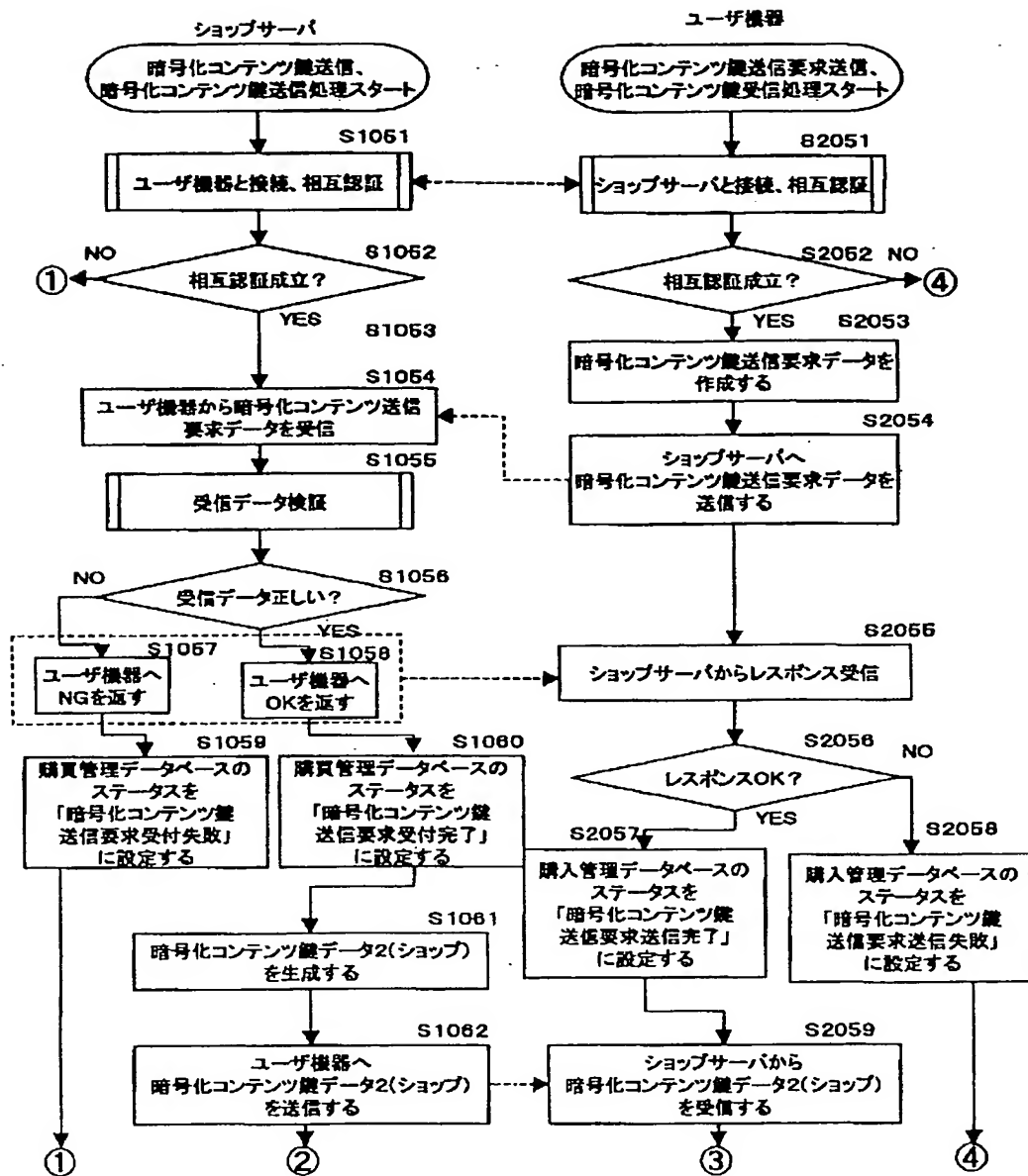
【図45】

チケット換金 サーバ処理No.	換金依頼元ID	チケット発行体ID	チケット発行 処理No.	金額	機器ID	ランゲージンID	ステータス
50001	12345	1234	10023	¥1000	1234567890	999888777	換金処理 レポート送信完了
50002	23450	4455	10455	¥250	2345678901	666555444	換金処理完了
50003	33201	2354	10254	¥800	345678901	321655444	電子チケット 受信完了

【図26】



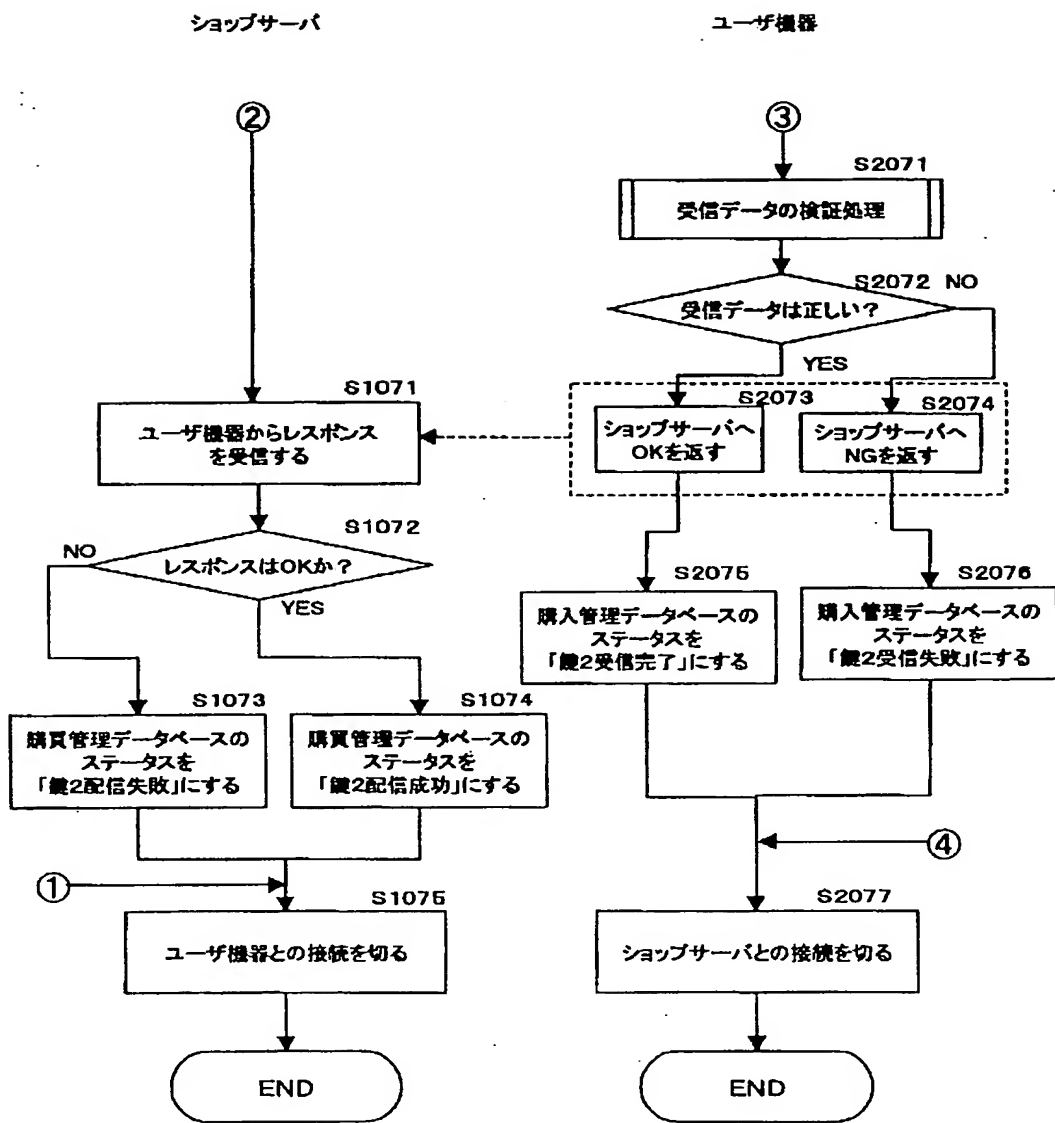
【図27】



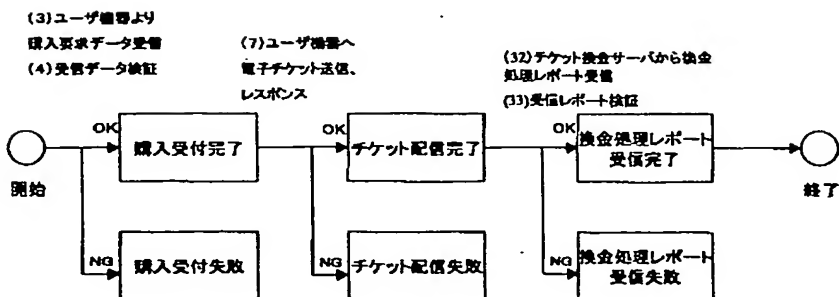
【図43】

配信サーバ 処理No.	コンテンツID	機器ID	チケット 発行体ID	チケット 発行処理No.	ステータス
999888777	5000	1234567890	1234	12345	換金処理 レポート受信完了
666555444	4050	3427781534	2345	23456	チケット換金要求 送信完了
999888779	5010	2355643551	1545	22335	配信完了
333555444	4320	4987390989	1030	32423	電子チケット 受信完了
2133545445	3232	3542416759	2253	44323	電子チケット 発信完了

【図28】



【図48】



The diagram illustrates the system architecture and data flow for a transaction process. The components and their interactions are as follows:

- User Device (ユーザ機器):**
 - Step (15) 受信データ検証 (Received Data Verification)
 - Step (16) 保存処理 $K_D \text{ DEV}(K_D) \rightarrow K_A$, $K_D \rightarrow K_{ATo}(K_C)$
- User Authentication Server (ユーザ認証サーバ (DAS)):**
 - Step (9) 受信データ検証 (Received Data Verification)
 - Step (10) 暗号化コンテンツ鍵かけかえ処理 $K_P \text{ DAS}(K_D) \rightarrow K_A$, $K_D \rightarrow K_P \text{ DEV}(K_D)$
- Shop Server (ショップサーバ (SHOP)):**
 - Step (11) 暗号化コンテンツ鍵データ(DAS)受信 (Received Encrypted Content Key Data from DAS)
 - Step (12) 受信データ検証 (Received Data Verification)
 - Step (13) 照合処理 (Verification Processing)
 - Step (14) 暗号化コンテンツ鍵データ(ショップ)送信 (Transmit Encrypted Content Key Data to Shop)
- Distribution Server (配信サーバ):**
 - Step (4) コンテンツ配信要求送信 (Transmit Content Distribution Request)
 - Step (5) 受信データ検証 (Received Data Verification)
 - Step (6) 暗号化コンテンツおよび暗号化コンテンツ鍵データ(配信サーバ)送信 (Transmit Encrypted Content and Encrypted Content Key Data to Distribution Server)
- Database (データベース):**
 - Stores K_D (Content), $K_P \text{ DAS}(K_C)$, and $K_P \text{ DEV}(K_C)$.
- Data Flows:**
 - 100:** From Shop Server to User Device.
 - 200:** From User Device to Shop Server.
 - 300:** From User Authentication Server to Shop Server.
 - 400:** From Shop Server to Distribution Server.

Figure 1 is a block diagram of a content distribution system. The system includes a User Equipment Server (DAS), a Shop Server (SHOP), a Distribution Server, and a User Equipment. The DAS and SHOP are connected via a network (100). The Distribution Server is connected to the SHOP via a network (400). The User Equipment is connected to the SHOP via a network (200). The DAS contains modules for (5) reception data check, (11) reception data check, (12) content encryption, (13) encrypted content data (DAS) transmission, (10) encrypted content data and encrypted content encryption key transmission, and (6) content distribution request transmission. The SHOP contains modules for (3) reception data check, (14) reception data check, (15) payment processing, (2) purchase request data transmission, (16) encrypted content data (Shop) transmission, and (17) reception data check. The Distribution Server contains modules for (7) reception data check and (8) encrypted content and encrypted content encryption key transmission. The User Equipment contains modules for (1) transaction ID and purchase request data generation, (9) reception data check, and (18) storage processing. A database (410) is connected to the Distribution Server and contains content keys (Kc) and DAS keys (Kd).

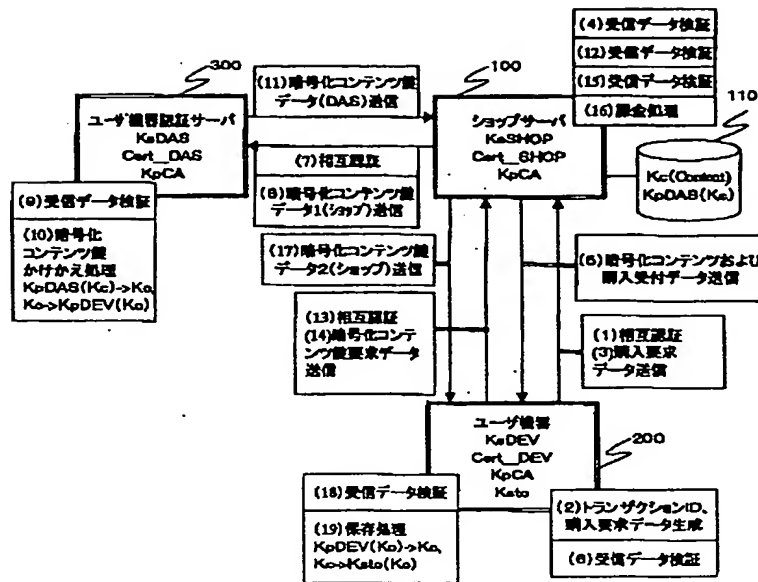
(22),(27)DAS、CPより
電子チケット受信
(23),(28)受信データ検証

(23),(28)換金処理

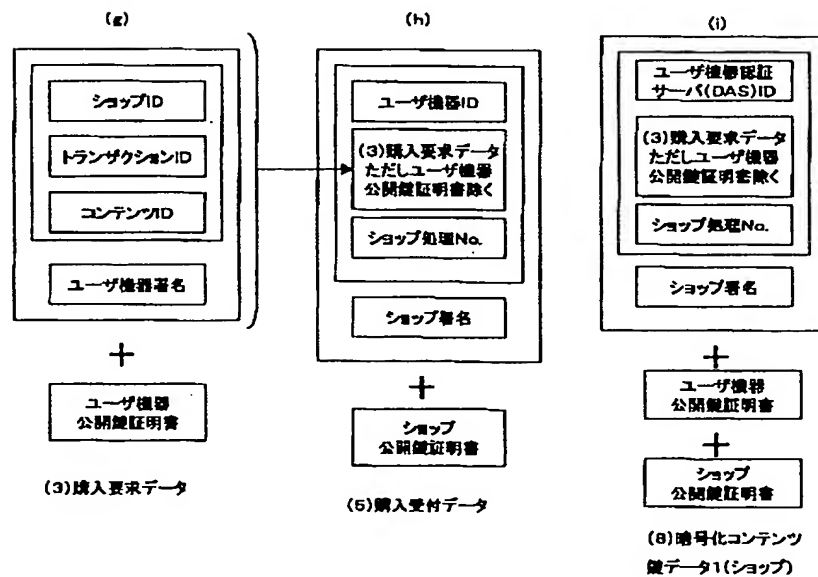
(24),(29)換金処理レポート送信、レスポンス

```
graph LR; Start((開始)) -- OK --> Step1[電子チケット受信完了]; Start -- NG --> Step1_NG[電子チケット受信失敗]; Step1 -- OK --> Step2[換金処理完了]; Step1 -- NG --> Step2_NG[換金処理失敗]; Step2 -- OK --> Step3[換金処理レポート送信完了]; Step2 -- NG --> Step3_NG[換金処理レポート送信失敗]; Step3 -- OK --> End((終了)); Step3 -- NG --> Step3_NG;
```

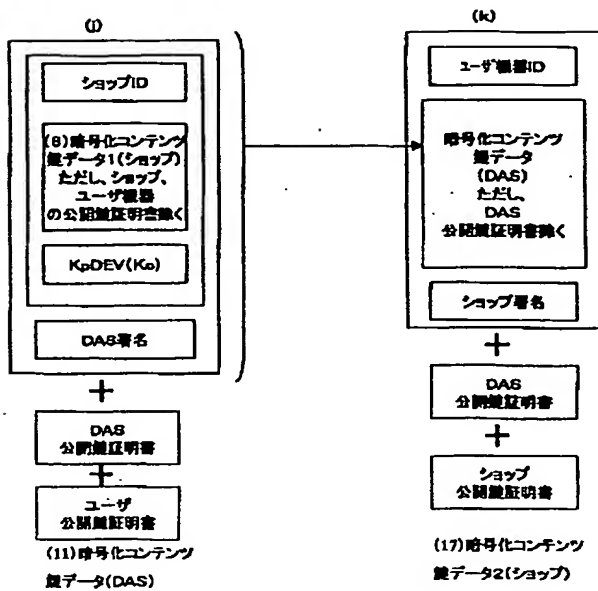
【図31】



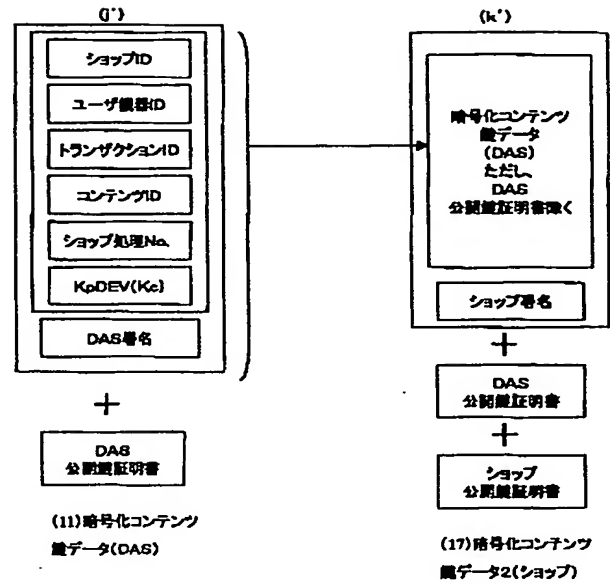
【図32】



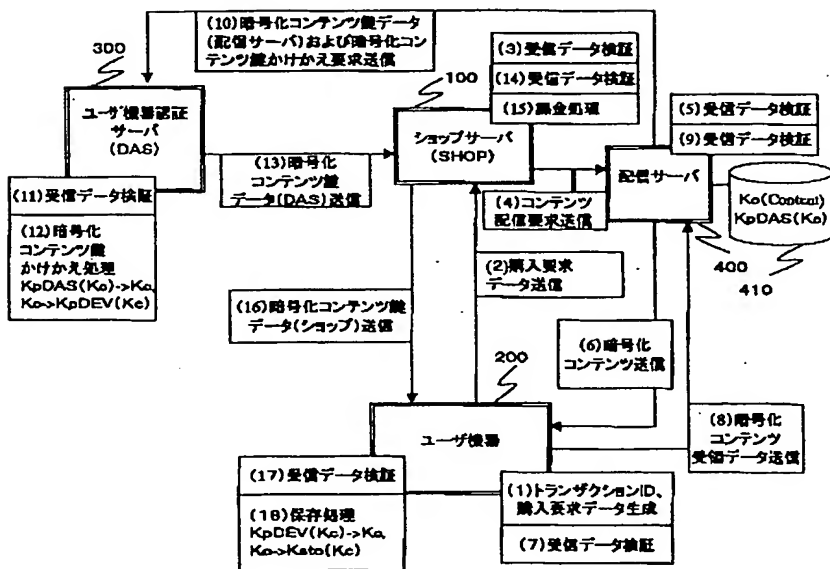
【図33】



【図34】



【図35】



【図76】

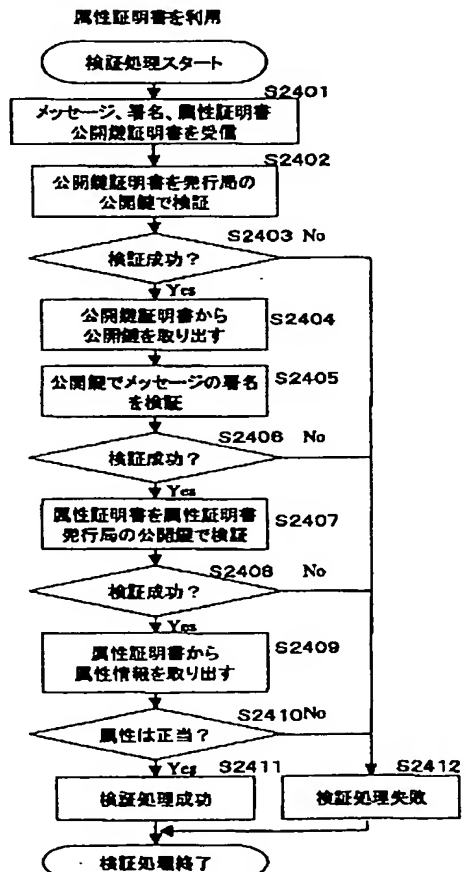


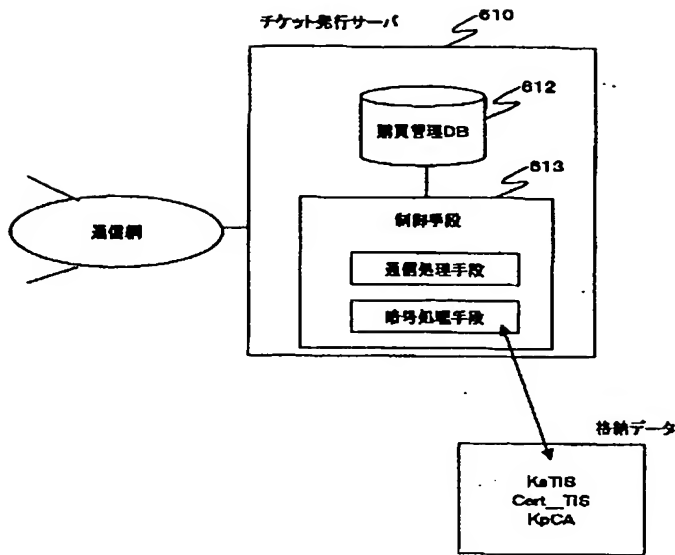
Figure 1 is a system architecture diagram illustrating the flow of data and control between a User Terminal, a Shop Server (SHOP), a User Authentication Server (DAS), and a Distribution Server. The diagram includes numbered steps (1) through (20) and labels for various data types and servers.

- User Terminal:**
 - (1) トランザクションID、購入要求データ生成
 - (9) 受信データ検証
 - (10) 暗号化コンテンツの受信データ送信
 - (19) 受信データ検証
 - (20) 保存処理 $KpDEV(Ka) \rightarrow Kc, Kc \rightarrow Kcat(Ka)$
- Shop Server (SHOP):**
 - (2) 購入要求データ送信
 - (3) 受信データ検証
 - (16) 受信データ検証
 - (17) 課金処理
 - (18) 暗号化コンテンツの店データ2(ショップ)送信
- User Authentication Server (DAS):**
 - (5) 受信データ検証
 - (13) 受信データ検証
 - (14) 暗号化コンテンツの暗号化鍵付け元処理 $KpDAS(Ka) \rightarrow Kc, Kc \rightarrow KpDEV(Kc)$
 - (15) 暗号化コンテンツの店データ(DAS)送信
- Distribution Server:**
 - (6) コンテンツ配信要求送信
 - (7) 受信データ検証
 - (11) 受信データ検証
 - (8) 暗号化コンテンツ送信
- Database:**
 - $Kc(Contest), KpDAS(Kc)$
- Control Flow:**
 - 300: Initial control flow from the User Terminal to the Shop Server.
 - 100: Control flow from the Shop Server to the User Authentication Server.
 - 200: Control flow from the Shop Server to the User Terminal.
 - 400: Control flow from the Distribution Server to the Shop Server.
 - 410: Control flow from the Distribution Server to the User Terminal.

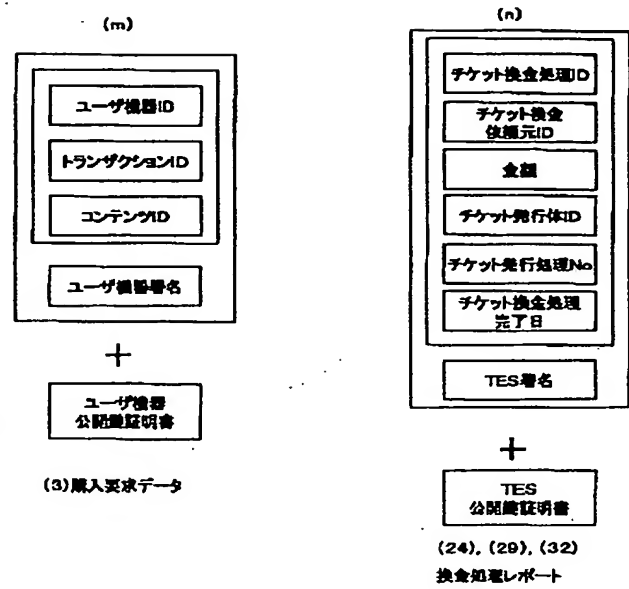
The diagram illustrates a system architecture for data exchange and security, involving several key components and their interactions:

- Central Servers:**
 - チケット授受サーバ (Ticket Issuance/Reception Server):** Contains $KaTES$, $Cert_TES$, and $KpCA$.
 - チケット発行サーバ (Ticket Issuance Server):** Contains $KaTIS$, $Cert_TIS$, and $KpCA$.
 - ユーザ情報:DEV (User Information:DEV):** Contains $KaDEV$, $Cert_DEV$, $KpCA$, and $Keto$.
 - ユーザ情報:サーバ (User Information:Server):** Contains $KaDAS$, $Cert_DAS$, and $KpCA$.
 - 配布サーバ (ex. コンテンツプロバイダ:CP) (Distribution Server (ex. Content Provider:CP)):** Contains $KaCP$, $Cert_CP$, and $KpCA$.
- External Components:**
 - データベース (Database):** Labeled $Kc(Oracal)$ and $KpDAB(Kc)$.
 - 外部サーバ (External Server):** Labeled $Kc(Oracal)$ and $KpDAB(Kc)$.
- Interactions and Data Flow:**
 - チケット授受サーバ ↔ チケット発行サーバ:**
 - (20) 相互認証
 - (27) 電子チケット (DAB用) 送信
 - (28) 授受データ検証, 授受処理
 - (29) 授受データ検証, 授受処理
 - (31) 相互認証
 - (32) 授受処理 レポート報告
 - チケット授受サーバ ↔ ユーザ情報:サーバ:**
 - (16) 受信データ検証
 - (17) 暗号化コンテンツ画かけえ処理
 - (18) $KpDAB(Kc) \rightarrow KpCA$
 - (19) $KpCA \rightarrow KpDEV(Kc)$
 - (30) 受信データ検証
 - チケット発行サーバ ↔ ユーザ情報:DEV:**
 - (7) 電子チケット (CP用, DAB用) 送信
 - (14) 相互認証
 - (15) 電子チケット (DAB用) および暗号化コンテンツ画かけえ要求送信
 - (18) $KpDAB(Kc)$ 送信
 - (19) 受信データ検証
 - (20) 授受処理 $KpDEV(Kc) \rightarrow KpCA$
 - (21) $KpCA \rightarrow Keto$
 - 配布サーバ ↔ ユーザ情報:DEV:**
 - (8) 相互認証
 - (9) 暗号化データ送信
 - (10) 電子チケット (CP用) 送信
 - (11) 暗号化コンテンツ, 暗号化コンテンツID, 暗号化コンテンツID, 暗号化コンテンツID
 - (12) 暗号化コンテンツID, 暗号化コンテンツID, 暗号化コンテンツID
 - (13) 暗号化データ検証
 - 外部データベース/サーバとの連携:**
 - チケット授受サーバ ↔ 外部データベース/サーバ:**
 - (21) 相互認証
 - (22) 電子チケット (CP用) 送信
 - (24) 授受処理 レポート報告
 - 配布サーバ ↔ 外部データベース/サーバ:**
 - (11) 受信データ検証
 - (25) 授受データ検証

【図38】



【図46】

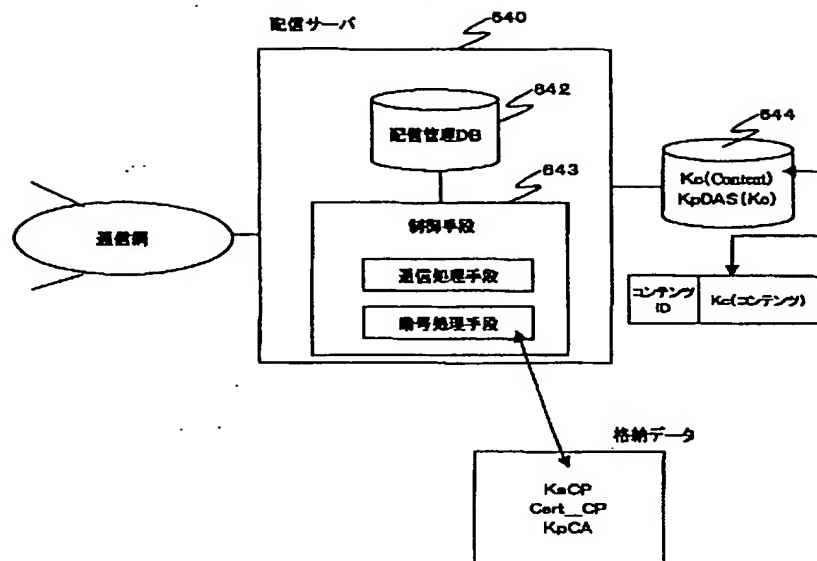


【図41】

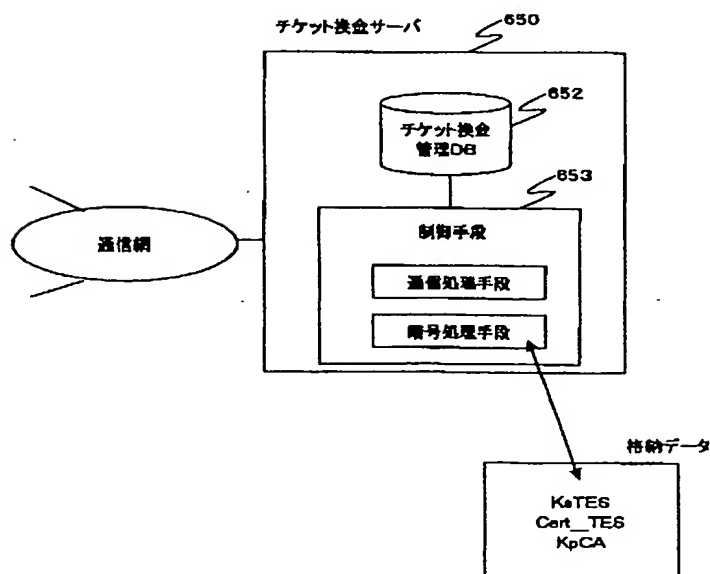
ユーザ機器保証サーバ処理No.	機器ID	トランザクションID	コンテンツID	チケット発行体ID	チケット発行処理No.	ステータス
50001	1234567890	999888777	5000	331234	10001	換金処理レポート受信完了
50002	2345678901	666555444	7050	345634	10025	チケット換金要求送信完了
50003	3456788901	321655444	8021	645234	10200	鍵送信完了
50004	5567778902	123555444	3245	321632	10325	鍵かけえ完了
50005	5435678445	335655321	2651	764545	12300	鍵受信完了

ユーザ機器保証サーバ・ライセンス管理DB

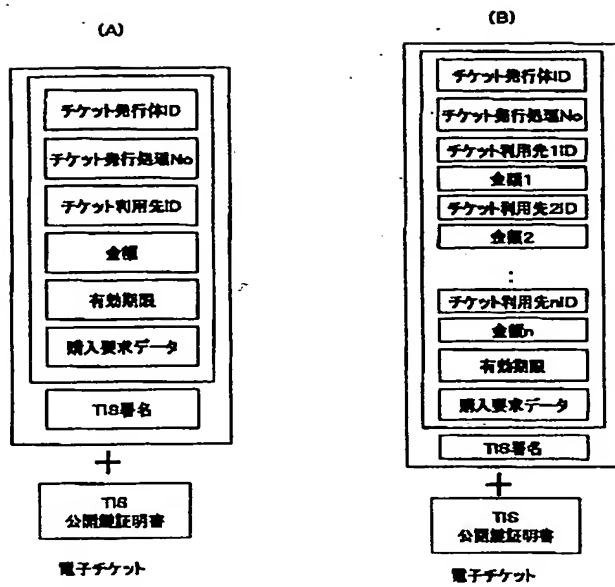
【図42】



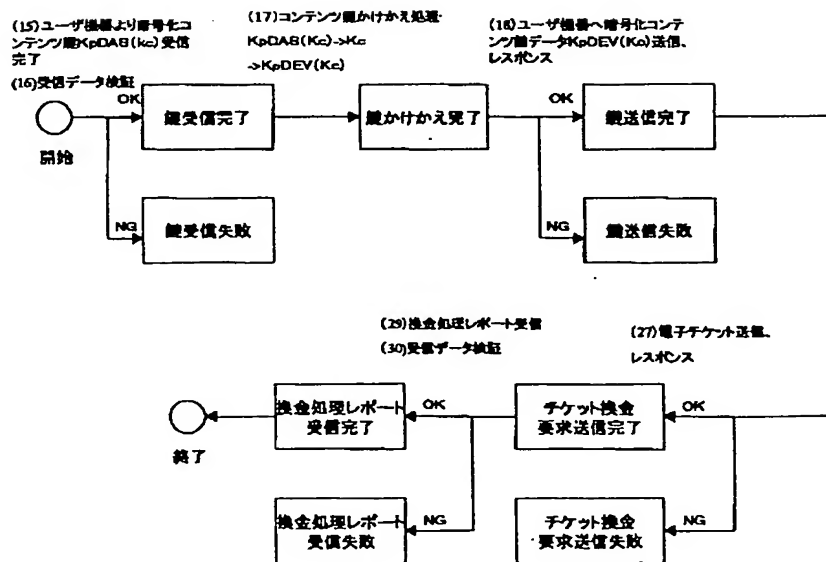
【図44】



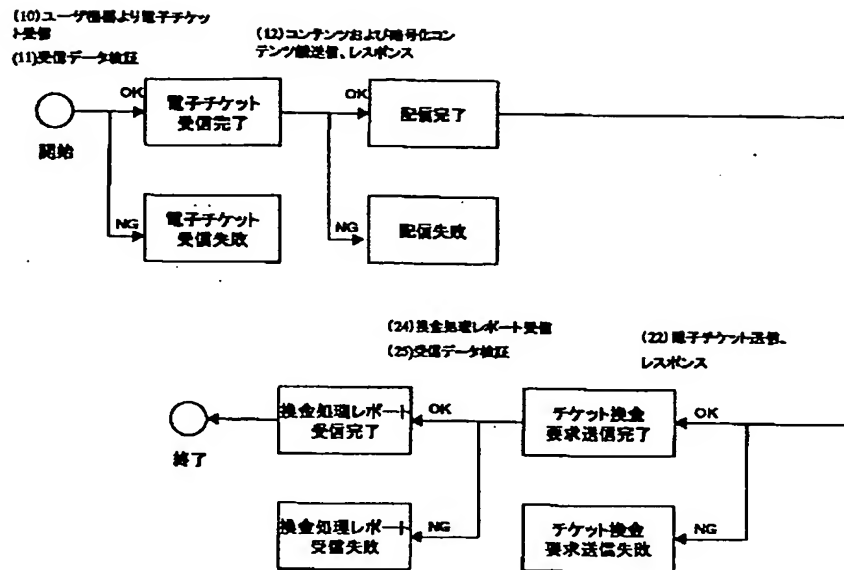
【図47】



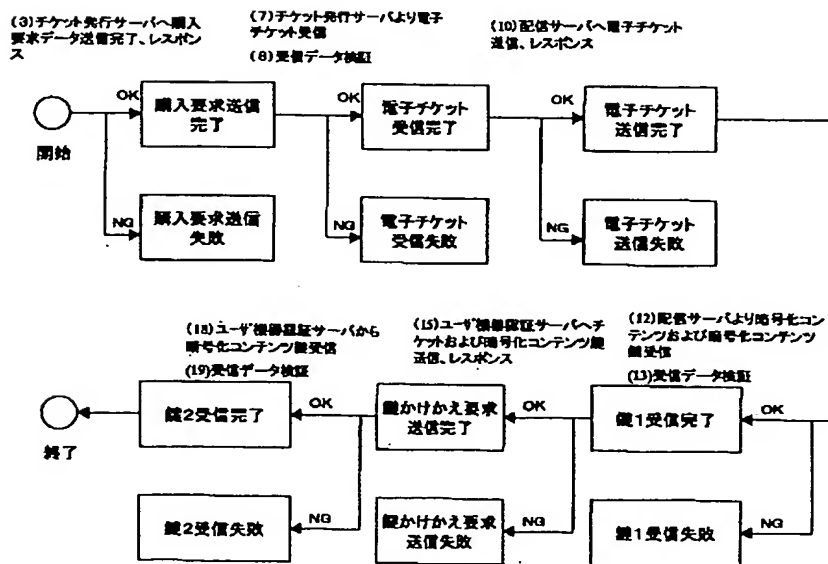
【図49】



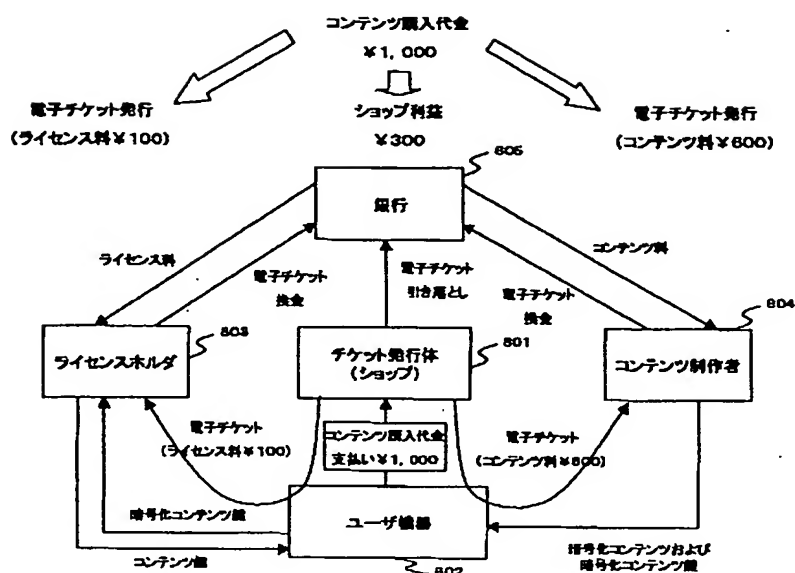
【図50】



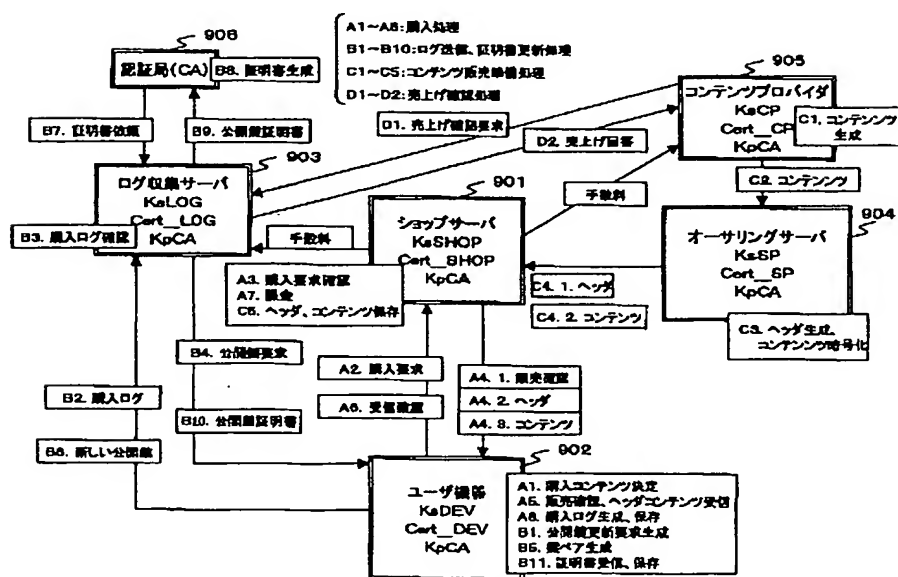
【図51】



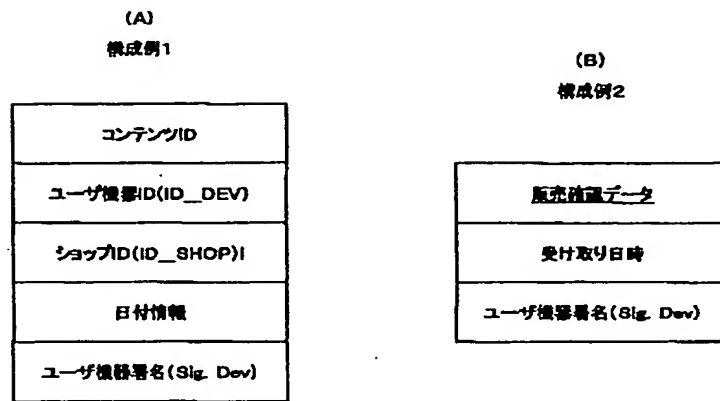
【図53】



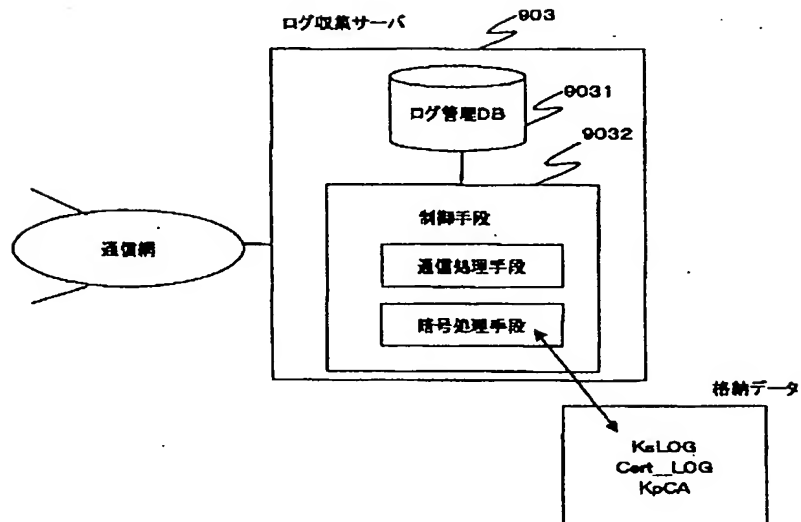
【図54】



【図55】



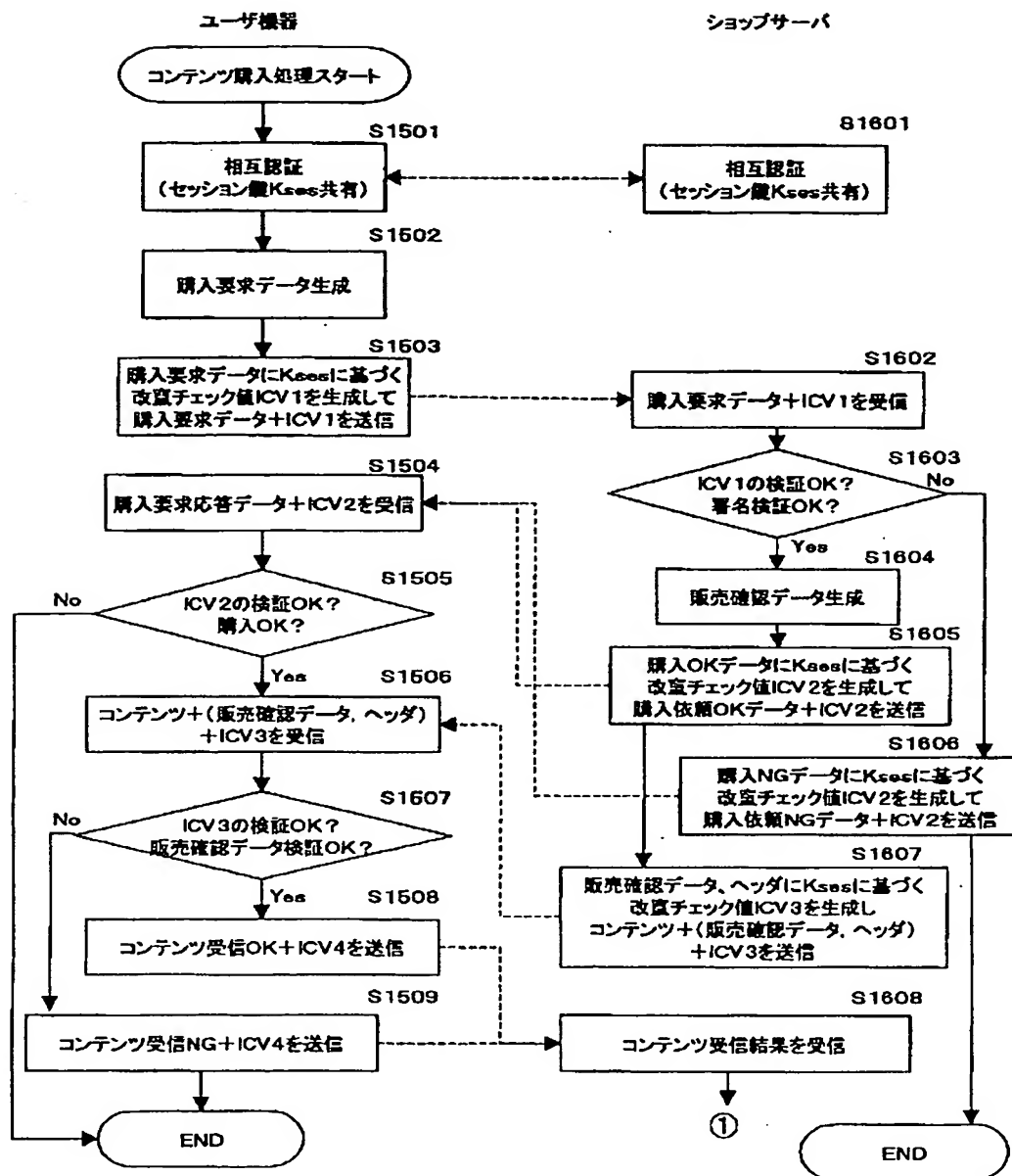
【図56】



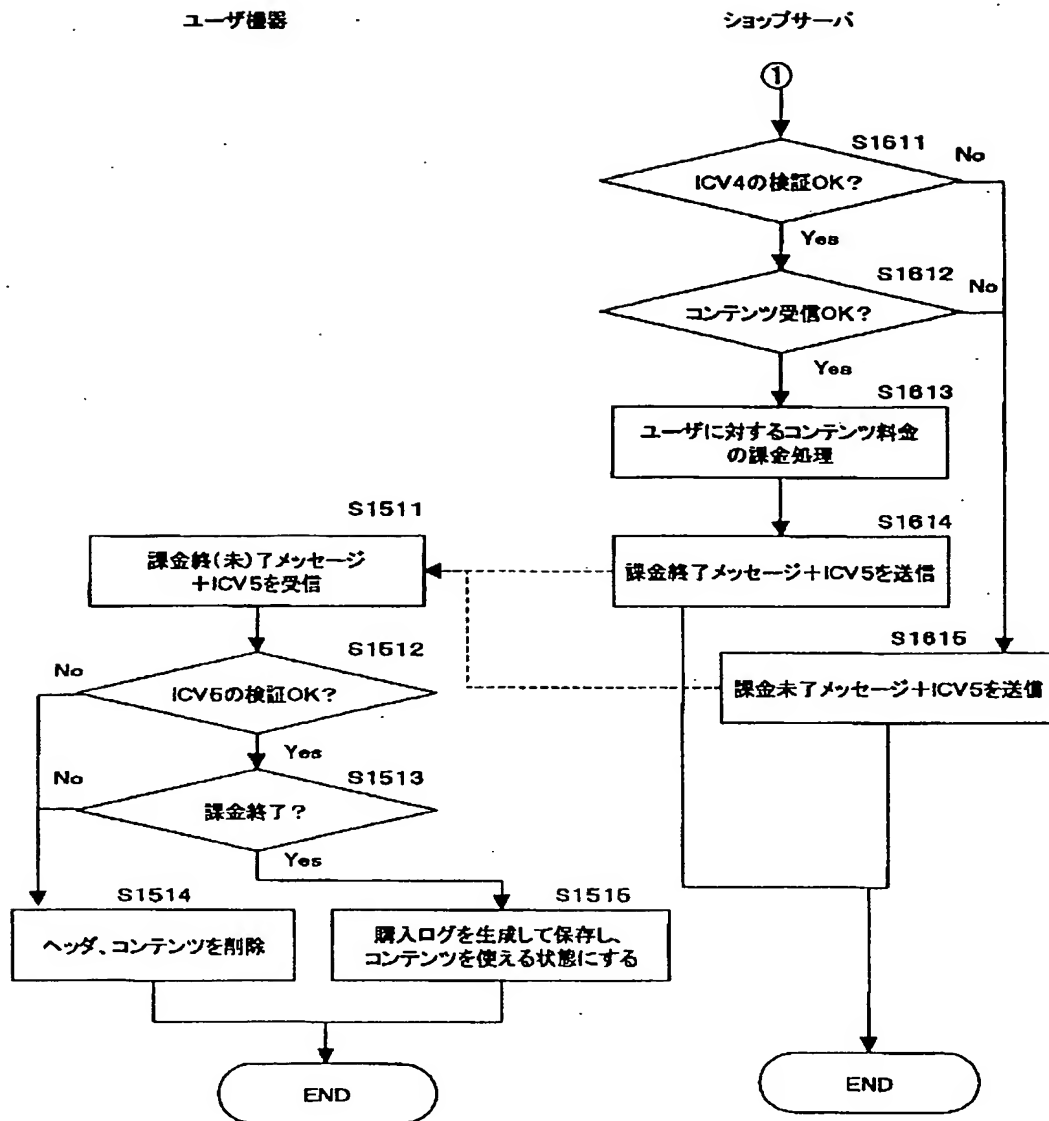
【図66】

属性コード(2バイト)	エンティティ	機能
0000	登録局(RA)	公開鍵証明書、属性証明書の発行審査を行なう
0001	サービス運営者(SH)	システム上で流通するコンテンツのライセンス料を徴収する or コンテンツを復号するタメの鍵のかけ替え処理、ログ情報の収集
0002	コンテンツ販売者(SHOP)	ユーザにコンテンツ内容を提供し、コンテンツ販売代金を徴収する
0003	コンテンツ配信者	コンテンツ販売者の要求に応じ、ユーザにコンテンツを配信する
0004	ユーザ機器	コンテンツの購入、利用を行なう
:	:	:

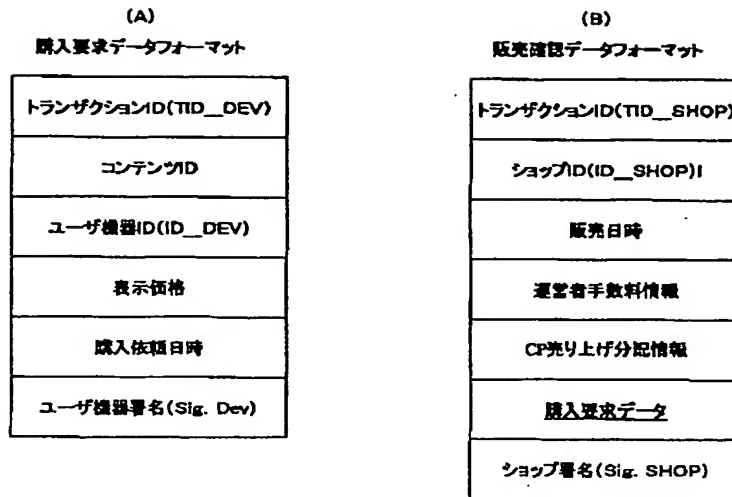
【図57】



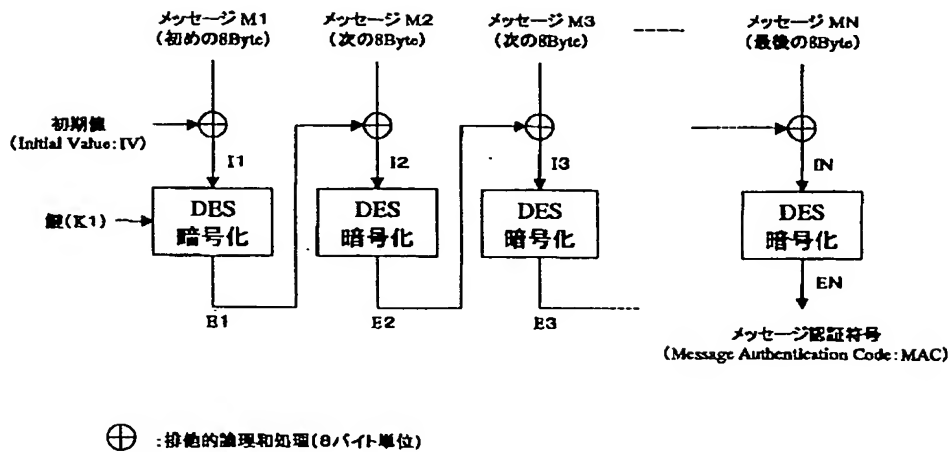
【図58】



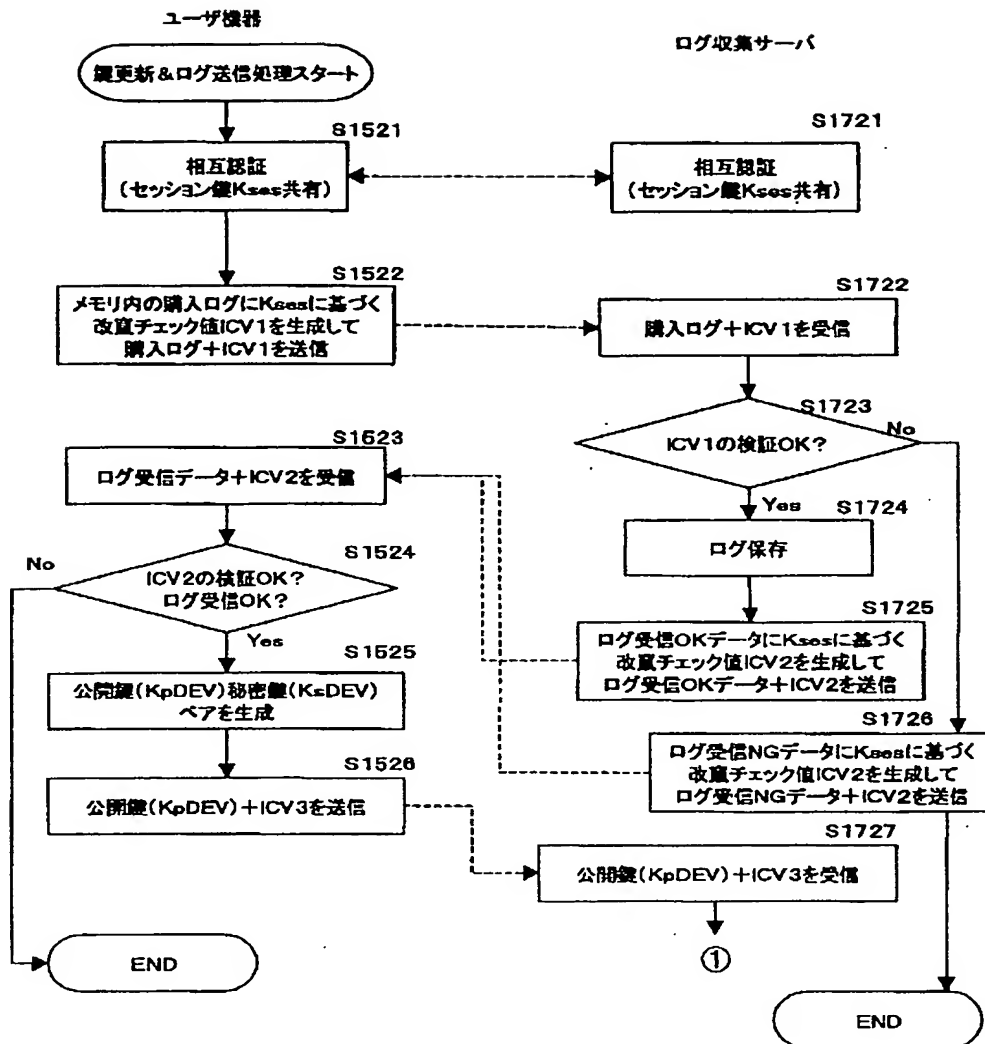
【図59】



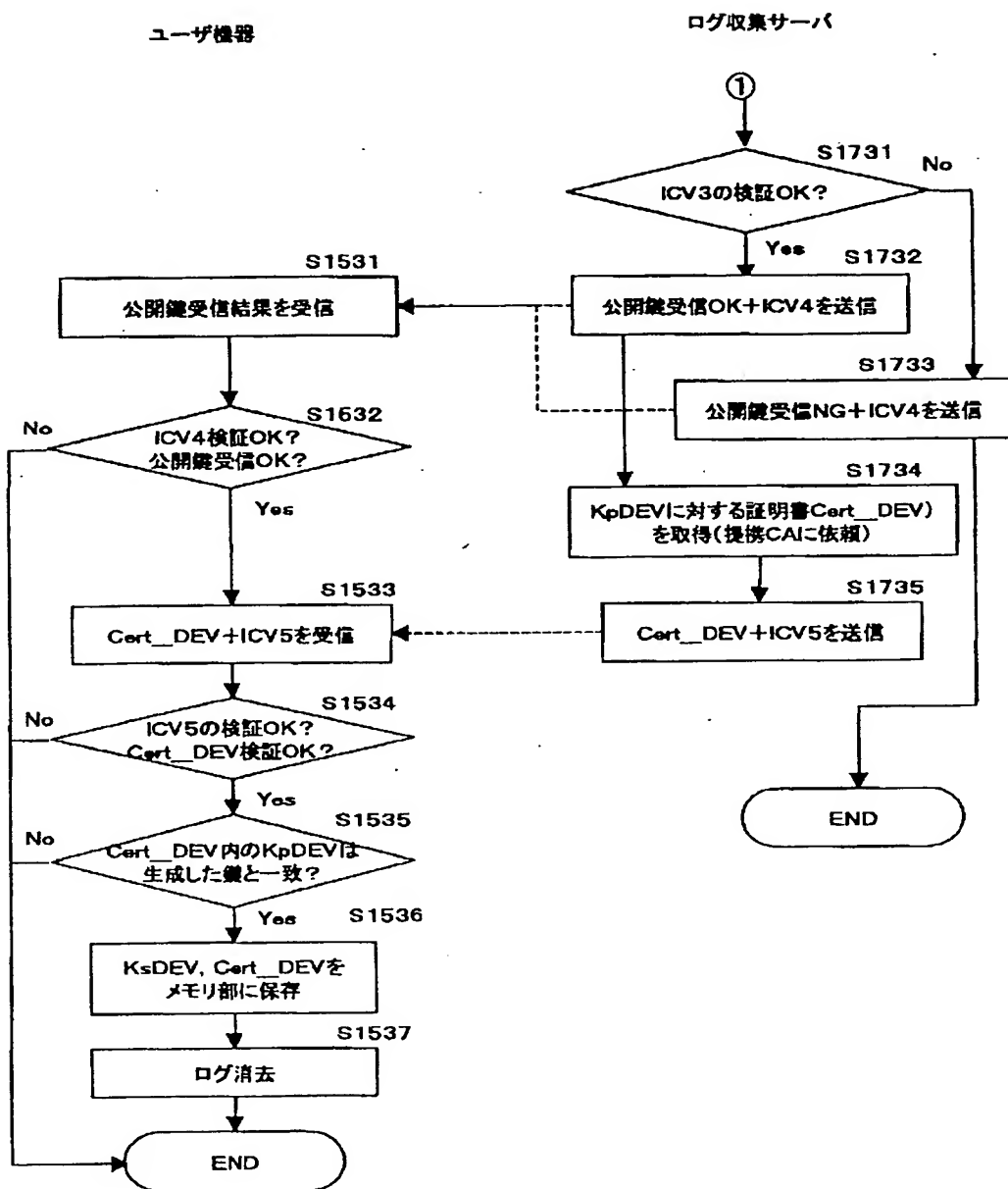
【図60】



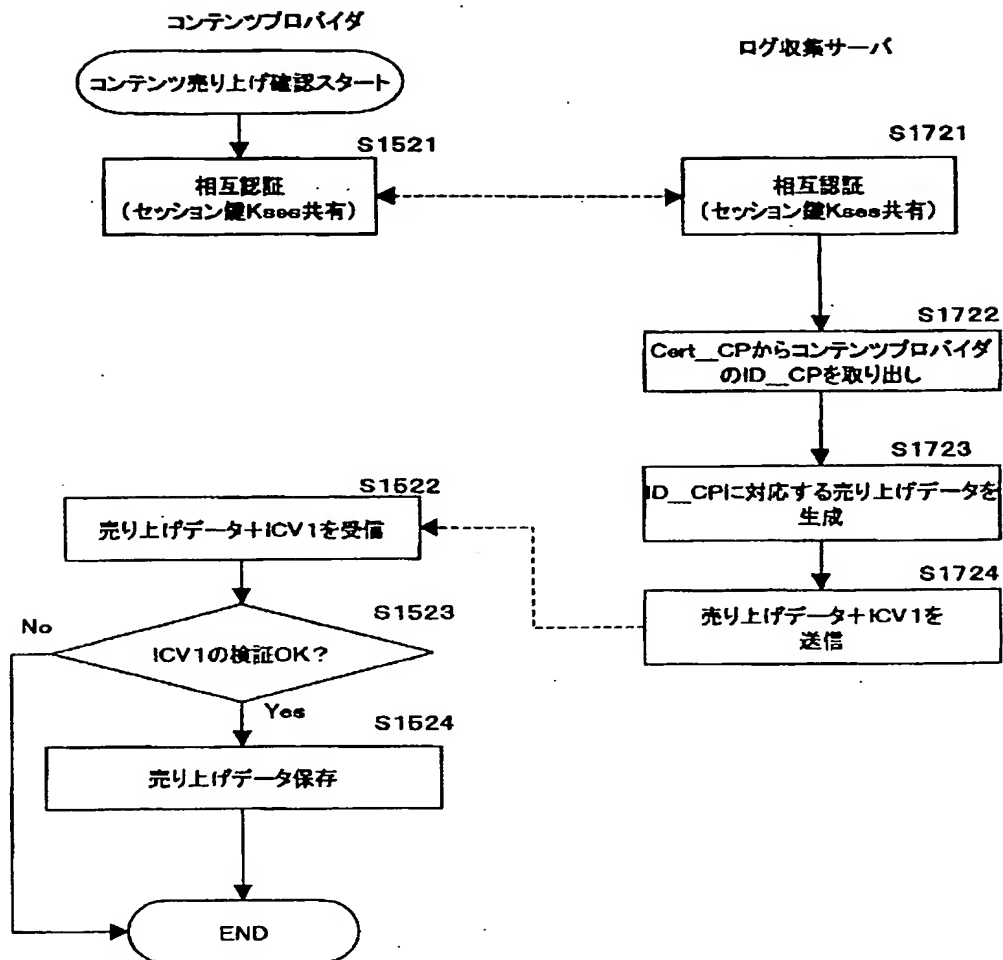
【図61】



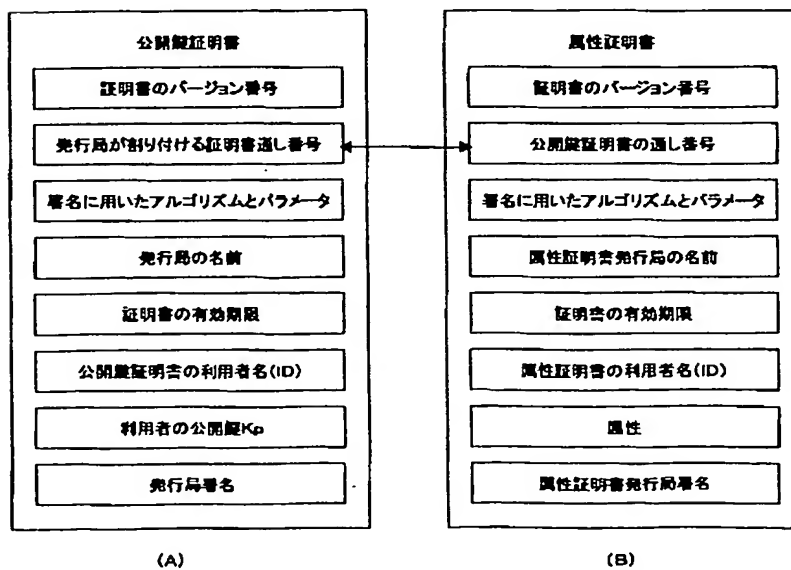
【図62】



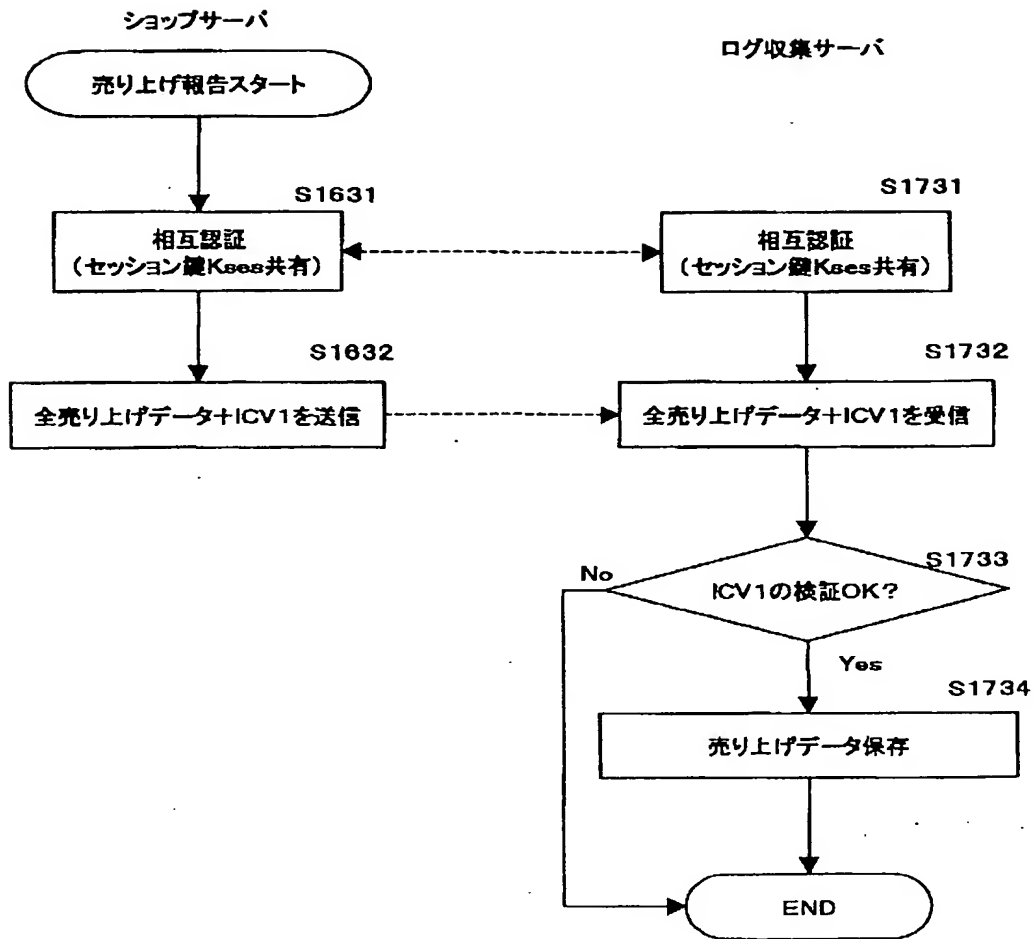
【図63】



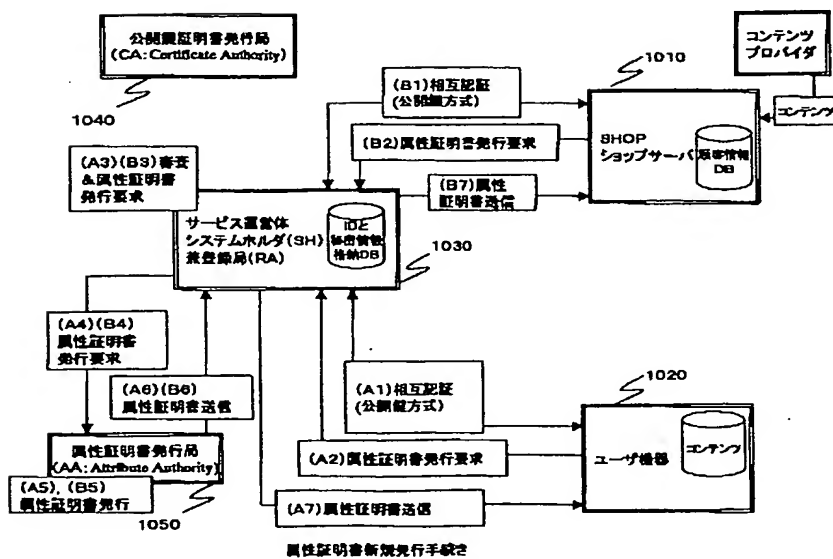
【図68】



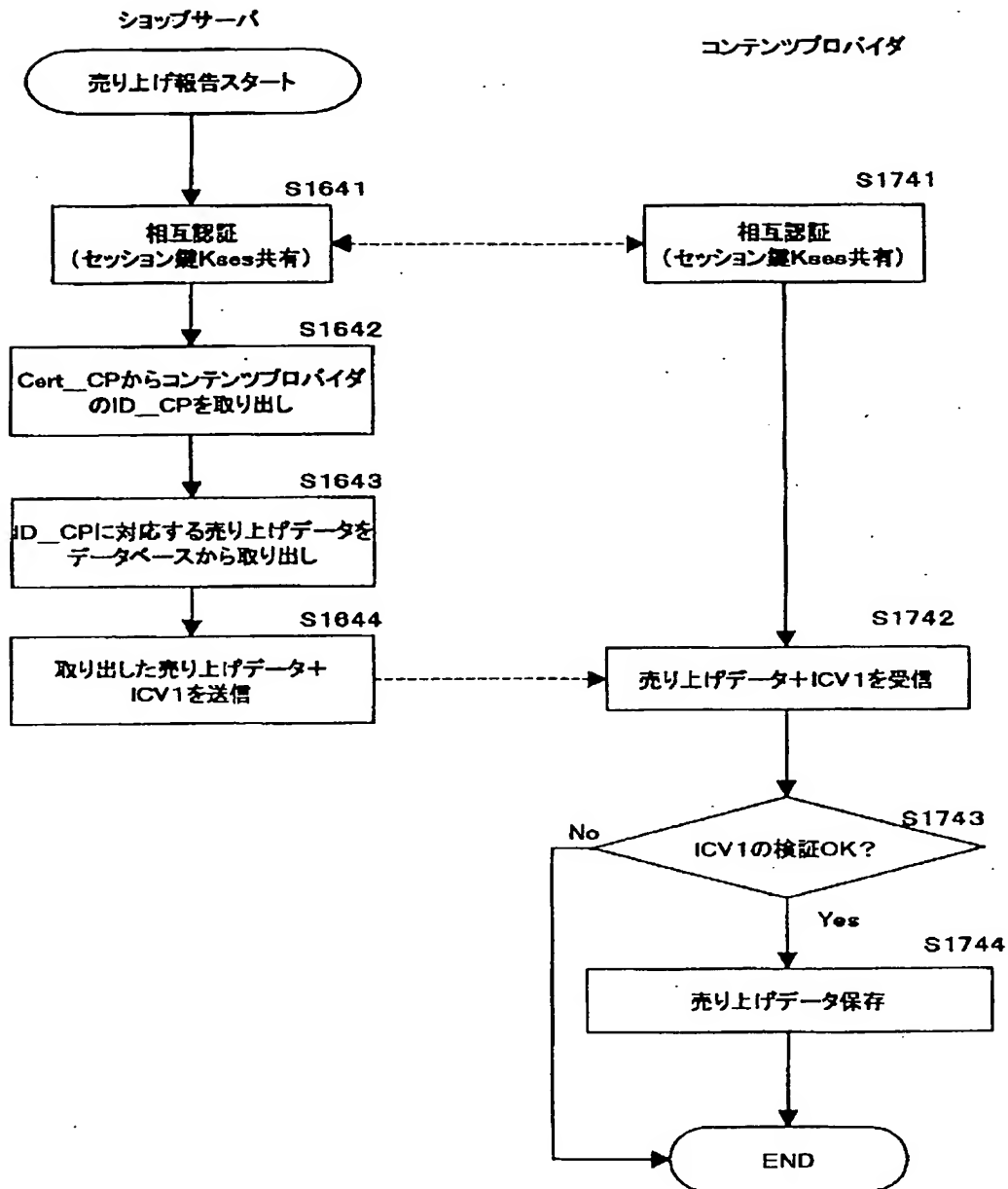
【図64】



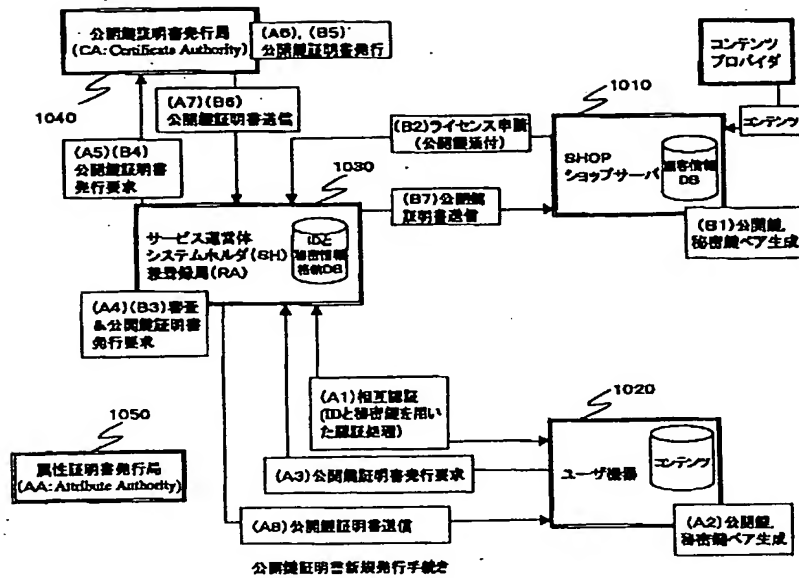
【図71】



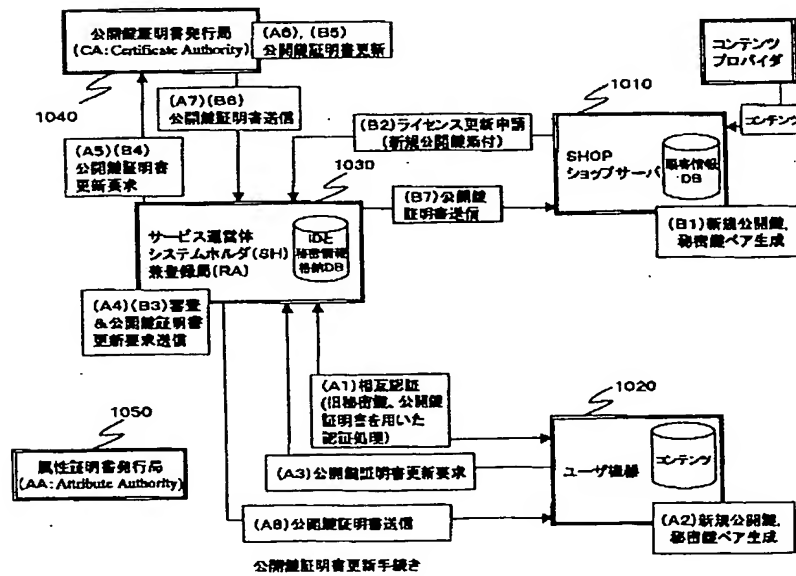
【図65】



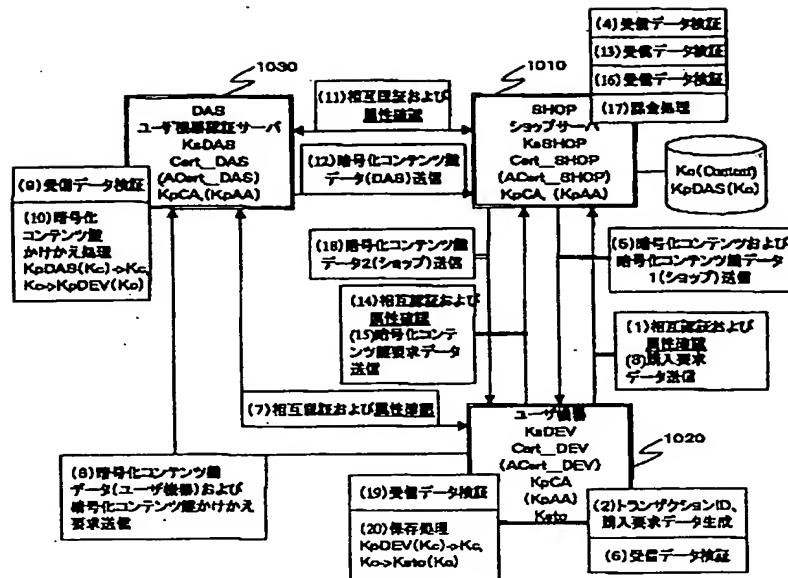
【図69】



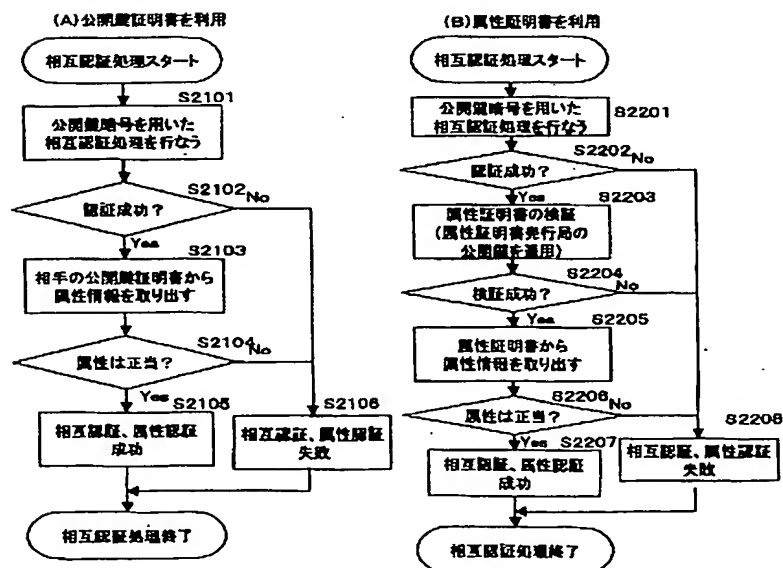
【図70】



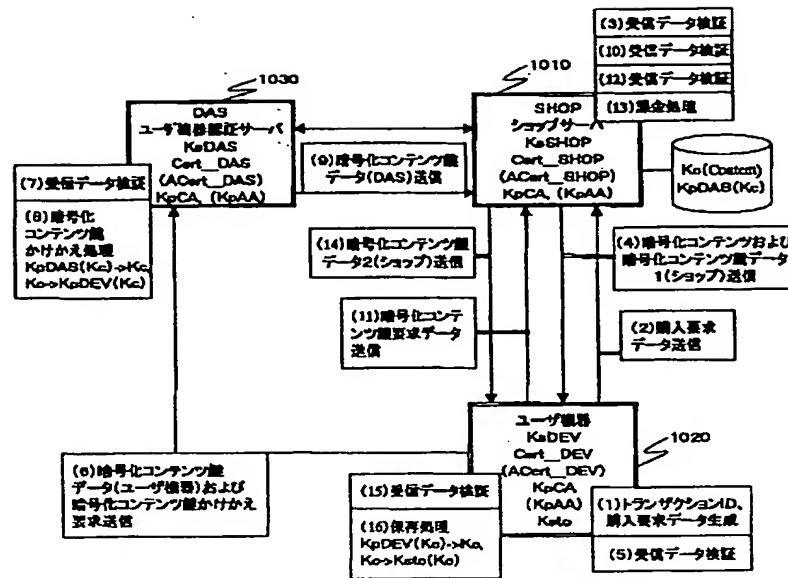
【図72】



【図73】



【図74】



フロントページの続き

(51) Int. Cl. 7	識別記号	F I	テーマコード* (参考)
G 0 6 F 17/60	3 1 0	G 0 6 F 17/60	3 1 0 E
	5 1 2		5 1 2
H 0 4 L 9/08		H 0 4 N 7/173	6 1 0 Z
9/32		H 0 4 L 9/00	6 0 1 C
H 0 4 N 7/167			6 7 5 B
7/173	6 1 0	H 0 4 N 7/167	Z

(72) 発明者 秋下 徹
 東京都品川区北品川6丁目7番35号 ソニ
 ー株式会社内

(72) 発明者 白井 太三
 東京都品川区北品川6丁目7番35号 ソニ
 ー株式会社内

(72) 発明者 岡 誠
 東京都品川区北品川6丁目7番35号 ソニ
 ー株式会社内

F ターム (参考) 5B049 AA05 BB00 CC05 DD01 EE01
 EE07 FF03 FF04 GG04 GG07
 GG10

5C064 BA01 BA07 BB05 BB07 BC07
 BC16 BC18 BC20 BC23 BC25
 BD02 BD07 BD08 CA14 CB01
 CC04

5J104 AA07 AA09 AA12 AA16 EA05
 EA06 EA18 EA19 KA02 KA05
 LA03 LA06 NA12 NA16 PA11

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.